Audit Report

PROGRAM MANAGEMENT OF THE
DEFENSE SECURITY SERVICE
CASE CONTROL MANAGEMENT SYSTEM

Report No. D-2001-019 December 15, 2000

Office of the Inspector General
Department of Defense

Additional Copies

To obtain additional copies of this audit report, visit the Inspector General, DoD, Home Page at: www.dodig.osd.mil/audit/reports or contact the Secondary Reports Distribution Unit of the Audit Followup and Technical Support Directorate at (703) 604-8937 (DSN 664-8937) or fax (703) 604-8932.

Suggestions for Future Audits

To suggest ideas for or to request future audits, contact the Audit Followup and Technical Support Directorate at (703) 604-8940 (DSN 664-8940) or fax (703) 604-8932. Ideas and requests can also be mailed to:

OAIG-AUD (ATTN: AFTS Audit Suggestions)
Inspector General, Department of Defense
400 Army Navy Drive (Room 801)
Arlington, VA 22202-4704

Defense Hotline

To report fraud, waste, or abuse, contact the Defense Hotline by calling (800) 424-9098; by sending an electronic message to Hotline@dodig.osd.mil; or by writing to the Defense Hotline, The Pentagon, Washington, D.C. 20301-1900. The identity of each writer and caller is fully protected.

Acronyms

CCMS	Case Control Management System
DSS	Defense Security Service

INSPECTOR GENERAL
DEPARTMENT OF DEFENSE
400 ARMY NAVY DRIVE
ARLINGTON, VIRGINIA 22202–4704

December 15, 2000

MEMORANDUM FOR ASSISTANT SECRETARY OF DEFENSE (COMMAND, CONTROL, COMMUNICATIONS, AND INTELLIGENCE)
DIRECTOR, DEFENSE SECURITY SERVICE

SUBJECT: Audit Report on Program Management of the Defense Security Service Case Control Management System (Report No. D-2001-019)

We are providing this report for review and comment. We conducted the audit in response to a congressional request. We considered management comments on a draft of this report when preparing the final report.

DoD Directive 7650.3, "Followup on General Accounting Office, DoD Inspector General, and Internal Audit Reports," September 5, 1989, requires that all unresolved issues be resolved promptly. Although the Assistant Secretary of Defense (Command, Control, Communications, and Intelligence) and the Defense Security Service concurred with the audit finding and recommendation, their management comments were incomplete. DoD Directive 7650.3 requires that management comments describe the corrective actions taken or planned, the completion dates of actions already taken, and the estimated dates for completion of planned actions. Therefore, we request that the Assistant Secretary of Defense (Command, Control, Communications, and Intelligence) and the Director, Defense Security Service, provide additional comments by January 18, 2001.

We appreciate the courtesies extended to the audit staff. Questions on the audit should be directed to Mr. Charles M. Santoni at (703) 604-9051 (DSN 664-9051) (csantoni@dodig.osd.mil) or Mr. David M. Wyte at (703) 604-9027 (DSN 664-9027) (dwyte@dodig.osd.mil). See Appendix F for the report distribution. The audit team members are listed on the inside back cover.

Robert J. Lieberman

Robert J. Lieberman
Assistant Inspector General
for Auditing

Office of the Inspector General, DoD

Report No. D-2001-019 **December 15, 2000**
(Project No. D2000AL-0159)

Program Management of the Defense Security Service Case Control Management System

Executive Summary

Introduction. This report discusses the program management of the Defense Security Service Case Control Management System in response to a request from the Chairmen of the Senate and House Committees on Armed Services. The Chairmen requested the review because of reported problems with processing security investigations for clearance determinations.

The Case Control Management System is an automated information system that guides and controls the Defense Security Service Enterprise System for opening, tracking, and closing personnel security investigation cases. The Enterprise System is a combination of 24 distinct primary information systems, subsystems, applications, and interfaces that share common data and connectivity.

The Defense Security Service believed that by establishing a paperless Enterprise System of automated applications, it would avoid as much as $80 million in operating costs and $900 million in reduced time for personnel security investigations. The Enterprise System did not meet performance expectations when it was deployed on October 28, 1998. Projected numbers of investigation case openings and closings did not materialize and times for investigations were not substantially reduced.

Objectives. The overall audit objective was to review the program management of the acquisition of the Defense Security Service Case Control Management System and the actions being taken to correct problems in its development and deployment. In addition, we evaluated the management control program related to the objective. See Appendix A for a discussion of the audit scope and methodology and the review of the management control program.

Results. The Defense Security Service did not effectively manage the high risk involved in the integration of the Case Control Management System and the Enterprise System. As a result, those systems had significant limitations and were insufficiently tested and evaluated for operational effectiveness prior to deployment in October 1998, leading to failures that degraded Defense Security Service productivity. As of September 2000, project management had been greatly improved, but high risks remained. Resolution of design problems is continuing and measurements for reliability and maintainability at production objectives are still needed.

The Air Force Program Management Office has developed a phased acquisition strategy to stabilize the Case Control Management System and the Enterprise System with product improvements and incrementally migrate it to an improved Enterprise System architecture between FY 2002 through FY 2008. However, the DoD needs to consider alternative solutions for processing personnel security investigations before further decisions are made on future system architecture.

The Defense Security Service appropriately identified personnel security investigations as a material management control weakness area in FYs 1999 and 2000, and is taking corrective actions. The DoD should continue to report management control weaknesses in this area until all overdue personnel security clearances requiring reinvestigation are eliminated. See the Finding section for details on the audit results and Appendix A for details on the DoD management control program.

Summary of Recommendations. We recommend that the Assistant Secretary of Defense (Command, Control, Communications, and Intelligence) and the Director, Defense Security Service, prior to making further decisions on the future system architecture, analyze whether the investment for the Case Control Management System and the Enterprise System provides the best business solution when compared to alternative solutions for opening, tracking, and closing personnel investigation cases.

Management Comments. The Assistant Secretary of Defense (Command, Control, Communications, and Intelligence) and the Director, Defense Security Service, concurred with the report finding and recommendation. A discussion of the management comments is in the Finding section of the report, and the text of the management comments is in the Management Comments section.

Audit Response. The Assistant Secretary of Defense (Command, Control, Communications, and Intelligence) and the Defense Security Service's comments were positive, but incomplete. The comments did not describe corrective actions taken or planned, dates of actions taken, and estimated completion dates of planned actions for implementing the recommendation. Therefore, we request that both the Assistant Secretary of Defense and the Director, Defense Security Service, provide additional management comments by January 18, 2001.

Table of Contents

Background

Personnel security investigations are essential for safeguarding classified resources. The Defense Security Service (DSS) manages and conducts these investigations for DoD. Annually, DSS closes more than 460,000 cases for clearance determinations by DoD central adjudication facilities.

In a March 14, 2000, letter to the Inspector General, DoD, the Chairmen of the Senate and House Armed Services Committees requested that a review be conducted of the recent reports regarding alleged problems with the DoD process for granting security clearances. Citing an October 27, 1999, General Accounting Office report that traced one of the causes to a DSS automated information system, the Chairmen requested the Inspector General, DoD, to review the problems that DSS experienced in the development and operation of the Case Control Management System (CCMS).

The CCMS is the automated information system that guides and controls the DSS Enterprise System of hardware and software applications for opening, tracking, and closing personnel investigation cases. The Enterprise System is a combination of 24 primary information systems, subsystems, applications, and interfaces that share common data and connectivity. The DSS believed that establishing a paperless Enterprise System would avoid as much as $80 million in operating costs and $900 million in reduced time for personnel security investigations. The Enterprise System did not meet performance expectations when CCMS was deployed on October 28, 1998.

Prior to the General Accounting Office report, several groups were invited to review the Enterprise System and suggest improvements. Reviews of the acquisition were performed by a DSS Integrated Program Team in March 1999, an Air Force/MITRE Red Team, and a DoD support contractor, TRW, Inc. The Deputy Assistant Secretary of Defense for Security and Information Operations tasked the contractor to conduct an analysis of program management and oversight of the Enterprise System. The TRW, Inc., report[1] made 37 short- and long-term recommendations for correcting and enhancing the system's performance.

In August 1999, the Air Force Standards System Group formally became the DSS Program Manager for the Enterprise System's development and operations. To improve and modernize the DSS Enterprise System, the Air Force Program Management Office prepared an acquisition strategy that it believed would stabilize the Enterprise System and incrementally migrates the system to a target architecture. The DSS FY 2002 Program Objective Memorandum programs funds to support this acquisition strategy through FY 2007.

[1]TRW, Inc., report, "TRW's Evaluation of the Defense Security Service's Case Control Management System," July 21, 1999.

The Assistant Secretary of Defense (Command, Control, Communications, and Intelligence) provides functional oversight for the DSS. Prior to September 2000, neither the CCMS nor the rest of the Enterprise System was designated as a major automated information system or a special interest initiative. Funds contractually obligated for the Enterprise System's development and modernization amounted to $76 million from FY 1995 through FY 1999. Total planned development and operation costs for FY 2000 through FY 2007 are estimated to be $312 million.

Objective

The overall audit objective was to review the DSS program management of the CCMS acquisition and the actions being taken to correct problems in its development and deployment. In addition, we evaluated the management control program related to the objective. See Appendix A for a discussion of the audit scope and methodology, prior coverage, and the review of the management control program.

The Case Control Management System and the Enterprise System

The DSS did not effectively manage the high risk involved in the integration of the CCMS and its Enterprise System. Those systems had significant limitations and were insufficiently tested and evaluated for operational effectiveness prior to deployment in October 1998, leading to failures that degraded DSS productivity. As of September 2000, project management had been greatly improved, but high risks remained. Resolution of design problems is continuing and measurements for reliability and maintainability at production objectives are still needed. In addition, DoD will need to consider alternative business solutions before making further decisions on the future system architecture.

Mandatory Guidance

The Clinger-Cohen Act of 1996, Office of Management and Budget Circulars, and DoD guidance for systems acquisition emphasize the importance of risk management when DoD organizations acquire information technology systems. Appendix B contains acquisition guidance for information technology systems.

Program Risk

Before deploying the CCMS in October 1998, DSS did not appreciate the technical and acquisition challenges involved with developing and deploying an information technology system with multiple interfaces. DSS did not implement effective risk management measures when it decided to become the system acquisition integrator and program manager for the Enterprise System. Further, despite the key role of the CCMS in DSS operations that support virtually all DoD critical missions, minimal acquisition oversight and guidance was provided or offered by the Assistant Secretary of Defense (Command, Control, Communications, and Intelligence). Also, DSS did not research and analyze alternative business processes to determine whether the DSS automated business function was the most cost-efficient and cost-effective solution for opening, tracking, and closing personnel security investigation cases prior to the development of the CCMS.

Technical Challenges. The Enterprise System deployed by the DSS in October 1998 had significant design limitations. The Enterprise System is a combination of linked internal and external information technology subsystems, many of which are derived from commercial-off-the-shelf hardware and software products. Specifically, CCMS, as the project management component of the Enterprise System, cannot open, track, or close investigation cases if the applications for workflow, scanning and printing, and interface links to the Defense Clearance and Investigations Index and corporate database do not function properly. Appendixes C and D provide a description of the Enterprise System and a diagram of the Enterprise System process.

Workflow. The sole-source acquisition and deployment of "Documetrix Workmanager," a commercial-off-the-shelf workflow application, proved to be a high-risk endeavor. "Documetrix Workmanager" required over 400 tasks to be sequentially accomplished before a personnel security investigation could be closed. When DSS deployed its Enterprise System, the sequential processing routine limited CCMS processing efficiency. Case analysts could not access the system to open investigation cases and define the work required. The DSS Integrated Process Team found that the CCMS with "Documetrix Workmanager" was taking four times longer to process cases than the paper-intensive process it replaced. A TRW, Inc., report described the "Documetrix Workmanager" as a major cause of CCMS inefficiency and operational problems.

Files Automation and Scanning Subsystem. The Files Automation and Scanning Subsystem, a commercial-off-the-shelf acquisition of hardware and software applications, also proved to be high risk. The Files Automation and Scanning Subsystem electronically passes paper and microfiche images to the CCMS applications for case openings and makes adjudication reports after case closures.

However, when DSS deployed the Enterprise System, the Files Automation and Scanning Subsystem failed to demonstrate operational effectiveness and reliability. The quality of electronic images passed to the CCMS was inconsistent and adjudication report processing was untimely. Further, DSS was aware of the scanning and printing anomalies. A list of more than 40 unresolved efficiency and reliability issues were submitted to the development contractor before the Enterprise System was deployed. As a result, when DSS went to a paperless operation, microfiche scans often had to be repeated. In addition, adjudication reports took an average of 9 weeks to print after case analysts closed the cases.

Defense Clearance and Investigations Index. After deploying the Enterprise System, DSS discovered that user access to and from the Defense Clearance and Investigations Index was being impeded. The Index could not process user clearance queries because the CCMS workflow application would continually return to the Index database searching for previously queried records. As a result, traffic to and from the Index increased and subsequently taxed the Index's ability to respond to customers' demands for information.

DSS Corporate Database. On June 29, 2000, the Enterprise System was shut down when a corporate database table reached its maximum capacity. The cause of the shutdown was a design limitation, because tables in the database could not exceed 4 million blocks of records. The DSS and the Air Force Program Manager were unaware of the block sizing limitation. The Air Force Program Manager and support contractors resolved the problem and operations were resumed on July 10, 2000.

Program Management. In developing and deploying the Enterprise System, DSS did not follow the systems acquisition guidance of the Office of Management and Budget and DoD addressing risk avoidance, reduction, and acceptance. Although analyses and plans concluded that the Enterprise System was a complex acquisition and involved risks, DSS personnel were not prepared to assume system acquisition management and integration responsibilities.

Analyses and Designs. Systems analyses and designs prepared in 1989 and 1994 identified the risks involved in the development of the CCMS and Enterprise System. In a May 1989 functional analysis document, a contractor described the CCMS and the Enterprise System as a large complex system that would take several years to develop and implement, and that database storage planning and design would be key elements that would affect the performance of Defense Investigative Service[2]-maintained databases. Further, the contractor recommended that the Defense Investigative Service include integration testing and parallel processing to mitigate risk.

The Defense Investigative Service's Strategic Implementation Plan, prepared in April 1994, described the CCMS case opening, tracking, and closing modernization as a massive development effort that far exceeded the Government's capability. Also, a Defense Investigative Service technical report described the modernization effort as a complex undertaking that should be incrementally acquired.

System Acquisition. Office of Management and Budget Circular A-109, "Major Systems Acquisitions," April 1976, implemented by DoD Directive 5000.1, "Defense Acquisition," March 15, 1996, requires that agencies engage skilled and experienced acquisition program managers for system solutions. Selected personnel should be knowledgeable in research and development, operations, engineering, testing, construction, contracting, prototyping, production, business, budgeting, and finance.

Further, the Circular provides seven objectives for managing systems acquisitions for avoiding, reducing, and accepting risks. Five of the seven objectives concern management controls. Specifically, acquiring organizations should:

- provide solutions that fulfill a mission need, operate effectively in intended environments, and demonstrate levels of performance and reliability that justify the investments,
- provide strong checks and balances by ensuring adequate system tests and evaluations, and conduct tests and evaluations independent of developers and users where practicable,
- accomplish acquisition planning resulting from clear articulations of agency mission needs,
- develop acquisition strategies that include test and evaluation criteria, methods for obtaining and sustaining competition in contracting, and methods for analyzing risks, and
- maintain capabilities to predict, review, assess, negotiate, and monitor life-cycle costs, assess experience against predictions, and report results of assessments to agency directors at key decision points.

[2]The Defense Investigative Service was renamed the Defense Security Service in November 1997.

Management Skills and Experience. Despite having been warned that its proposed information technology system for managing personnel security investigations was high risk, DSS developed the system without researching and analyzing whether alternative functional solutions for opening, tracking, and closing investigation cases existed for its business process. Assuming program management and systems integration responsibilities for the information technology acquisition, DSS did succeed in assembling a workable product. However, the product obtained with Government-wide acquisition contracts from hardware and software contractors was flawed, and according to TRW, Inc., "At best, the DSS Enterprise System is a working prototype."

As the system program manager and integrator, DSS personnel did not have the requisite training or experience in acquiring and integrating automated information systems. The design, reliability, and maintainability discrepancies discovered after the system was deployed can be traced to personnel lacking experience and skills in research and development, operations, engineering, testing, construction, contracting, prototyping, production, business, budgeting, and finance. Such skills are obtained through structured classroom and on-the-job training. As concluded by TRW, Inc., "Overall, [CCMS] looks like a business example for how not to do a system acquisition."

Test and Evaluation. DSS did not stress test the CCMS and the Enterprise System for opening, tracking, and closing investigation cases before deploying it. Specifically, DSS did not deliberately try to "crash" the system to determine its threshold limits and did not perform prolonged operational tests to determine system reliability and maintainability.

Tests conducted prior to system deployment demonstrated only the functionality of the CCMS and the Enterprise System and did not demonstrate its effectiveness and suitability in an operational environment. As a result, DSS did not identify unknown defects, such as the inaccessibility of the Defense Clearance and Investigations Index and the limitations of sequential processing. Further, DSS could not project the extent of known design limitations with the Files Automation and Scanning Subsystem and the corporate database.

Life-Cycle Costing. DSS did not cost out the phases of the Enterprise System acquisition from development through disposal. Planned functions and tasks were not identified by fiscal years over the system's acquisition life. As a result, funds for acquiring the Enterprise System did not translate operational needs and requirements into an information technology solution or identify resources for operating and maintaining the deployed system.

Project Monitoring. DSS did not monitor the CCMS and Enterprise System acquisition to review, assess, predict, and report results. Without a life-cycle baseline for the system's acquisition phases, cost, schedule, and performance comparisons for measuring progress, computing deviations, and projecting results could not be determined.

DSS measured progress in acquiring the CCMS and the Enterprise System based on fiscal year resources and obligated funds. The CCMS and the Enterprise System could not be tested and evaluated in an operational environment for effectiveness and suitability because available funds were not programmed for a test facility.

Documentation. DSS deployed the CCMS and the Enterprise System without testing the design configuration and operating documentation. By not conducting prolonged operational tests and evaluations to determine whether the automated information systems could be safely recovered and returned to service after failures, DSS did not know whether the systems could be suitably maintained. The TRW, Inc., report stated that it was "imperative" for DSS to develop an operations plan for resolving system bottlenecks and identifying sources of inefficiencies and malfunctions.

TRW, Inc., also identified additional program baseline documentation required for effectively and efficiently maintaining and sustaining the CCMS and the Enterprise System. Specifically, TRW, Inc., indicated that reports and analyses were needed to address concept of operations, system requirements specifications, interface control definitions and maintenance plans.

Program Oversight

The Clinger-Cohen Act requires Chief Information Officers to monitor and evaluate the performance of information technology programs and advise the heads of agencies whether to continue, modify, or terminate a program. The Office of Assistant Secretary of Defense (Command, Control, Communications, and Intelligence), the DoD Chief Information Officer, did not actively participate in the acquisition of the DSS Enterprise System because costs of the investment fell below cost thresholds[3] established for classification as a major automated information system. In addition, as the Principal Staff Assistant responsible for the development, oversight, and integration of DoD policies and programs relating to security, the Office of the Assistant Secretary of Defense (Command, Control, Communications, and Intelligence) should have exercised acquisition oversight over DSS and chose not to do so. As a result, DSS was allowed to develop, deploy, and operate the CCMS and the Enterprise System for personnel security investigations without the benefit of program oversight and guidance.

[3]Major automated information systems are estimated to require program costs in any single year in excess of $30 million (FY 1996 constant dollars), and total program costs in excess of $120 million (FY 1996 constant dollars), or total life-cycle costs in excess of $360 million (FY 1996 constant dollars).

Since March 1999, the Assistant Secretary of Defense (Command, Control, Communications, and Intelligence) has been more proactively involved with the DSS information technology acquisition. The Assistant Secretary planned to subject the DSS Enterprise System to DoD Directive 5000.1 acquisition guidance by designating it as a major automated information systems acquisition when he releases the revised list of designated major automated information system acquisition and special interest initiative programs.

Prior Report Recommendations

Recommendations from the Air Force/MITRE Red Team[4] and a report from TRW, Inc., ranged from establishing a program management office to system replacement and maintenance. Ranked by short-term and long-term significance, DSS was using these recommendations for follow-up and progress reporting on the General Accounting Office report's[5] recommendation to correct the CCMS. See Appendix E for the TRW, Inc., recommended actions and the progress DSS made in addressing them. In addition, DSS processed a CCMS change request to account for security investigations from request to case closure as a result of Inspector General, DoD, Report No. D-2000-134, "Tracking Security Clearance Requests," May 30, 2000.

Management Activities

Following the Red Team and TRW, Inc., recommendations, DSS began modifying its deployed automated information systems and baselining its system acquisition for Clinger-Cohen Act certification by the DoD Chief Information Officer. Since the Air Force and its contractors assumed program and functional responsibilities for the Enterprise System, DSS has made production advances in achieving its performance goal of closing more than 50,000 investigations per month. From December 1999 through June 2000, case closure rates increased from 19,561 to 38,374 investigations per month.

However, design limitations exist and demonstrated reliability and maintainability at planned production goals remain to be determined. The Files Automation and Scanning Subsystem improvements still require continuous human supervision for processing and printing paper documents. Also, the corporate database could shut down the DSS Enterprise System if closed investigations cases are not removed and archived. Further, closed investigations remaining in the database affect case processing efficiency by extending time required for opening, tracking, and closing active investigations.

Although DSS was aware of the corporate database design limitation when the Enterprise System was deployed, DSS did not consider it a high priority.

---

[4]Air Force/MITRE Red Team report, "Red Team Recommendations-Transition Ahead," July 14, 1999.

[5]General Accounting Office Report No. NSIAD-00-12, "Inadequate Personnel Security Investigations Pose National Security Risks," October 27, 1999.

However, as the cases processed increase, the database design limitation becomes an increasing concern. For example, the number of cases in process on June 30, 2000, was 433,620 compared to 337,378 on December 31, 1999. Further, the number of cases in process for more than 360 days was 69,260 on June 30, 2000, compared to 14,242 on December 31, 1999.

As of April 2000, the corporate database contained 26 million records for opened and closed cases. System efficiency could be significantly increased if inactive records populating the database could be removed and archived. DSS and the Air Force Program Management Office are aggressively taking action to reduce the records in the Enterprise System's corporate database. The Air Force Program Management Office estimates that 25 million records could be removed from the corporate database and archived.

Analysis of Alternatives

The Air Force Program Management Office developed a phased acquisition strategy for maintaining and modernizing the CCMS and Enterprise System. The strategy involved introducing product improvements that will incrementally migrate it to an improved system architecture from FY 2002 through FY 2008. The strategy did not include an analysis of alternatives because the Air Force Program Management Office assumed that the business function for opening, tracking, and closing investigation cases would remain a DSS mission responsibility.

Clinger-Cohen Act. Public Law 104-106, Division E, "Clinger-Cohen Act," sections 5113 and 5123, "Performance and Results-Based Management," requires agency heads to make decisions that affect information technology investments. Before investing in a new information system, heads of each executive agency are to determine whether the function in need of automation should be performed by the executive agency and, if so, whether the function should be performed by a private sector source under contract or by executive agency personnel. Also, the Act requires that agency heads analyze missions and, based on the analysis, revise mission-related processes and administrative processes, as appropriate, before making significant investments in information technology.

Other Investigative Sources. Alternative automated business processes for managing personnel investigations may exist for opening, tracking, and closing personnel investigation cases. DSS plans to outsource more than 1 million requests for security investigation cases, or 30 percent of its estimated workload, to the Office of Personnel Management and private-sector contractors between FY 2000 and FY 2003. Although DSS will maintain accountability, the forwarded cases will not be opened and tracked in the CCMS and the Enterprise System. The Office of Personnel Management and the private-sector contractors will be responsible for managing the case investigations they receive and for maintaining project management systems for opening, tracking, and closing assigned cases.

Because alternative business processes for managing personnel investigations will be employed by the Office of Personnel Management and private-sector contractors, we believe the Assistant Secretary of Defense (Command, Control, Communications, and Intelligence) and DSS should reassess whether the CCMS and the Enterprise System provide the most efficient and effective business solution. DoD personnel security clearance requirements that drive DSS workload investigation cases have been addressed by an integrated product team established by the Deputy Secretary of Defense to review the DoD personnel security investigation process. Alternative solutions have also been discussed at meetings with Government and contractor personnel familiar with the business process. Further, the Deputy Assistant Secretary of Defense for Security and Information Operations stated before a congressional subcommittee that alternatives would be analyzed before DoD commits to a future architecture.[6] However, we found no indication of formal in-depth analysis of alternatives.

Conclusion

DSS deployed the CCMS and its Enterprise System for opening, tracking, and closing investigation cases in October 1998 without first demonstrating system operational effectiveness and suitability. By not managing risks with accountable links to program definition, structure, design, assessments and reports, and oversight decision reviews, DSS acquired the CCMS and the Enterprise System with known and unknown design, reliability, and maintainability limitations. As of September 2000, DSS and the Air Force Program Management Office had restored system acquisition discipline. However, design inefficiencies still exist, and reliability and maintainability at planned production objectives still need to be demonstrated.

The Assistant Secretary of Defense (Command, Control, Communications, and Intelligence) plan to designate the CCMS and the Enterprise System as a Major Automated Information System is a positive development. Further, the Deputy Assistant Secretary of Defense for Security and Information Operations indicated that alternatives would be analyzed before DoD commits to a future architecture. Action is needed now to lay groundwork for future decisions that need to consider alternatives for the CCMS and the Enterprise System target architecture. Because alternative Government and private-sector systems exist that may provide efficient and effective solutions for opening, tracking, and closing investigation cases, the target architecture needs to be reassessed to determine its validity.

[6]Testimony to the Subcommittee on National Security, Veterans Affairs, and International Relations, House Committee on Government Reform, September 20, 2000.

Recommendation, Management Comments, and Audit Response

We recommend that the Assistant Secretary of Defense (Command, Control, Communications, and Intelligence) and the Director, Defense Security Service, prior to making further decisions on the future system architecture, analyze whether the investment for the Case Control Management System and the Enterprise System provides the best business solution when compared to alternative solutions for opening, tracking, and closing personnel investigation cases.

Management Comments. The Assistant Secretary of Defense (Command, Control, Communications, and Intelligence) and the Director, Defense Security Service, concurred with the recommendation. In addition, The Director attached a matrix to his comments with suggested editorial corrections to the report.

Audit Response. The Assistant Secretary of Defense (Command, Control, Communications, and Intelligence) and the Defense Security Service comments were positive, but incomplete. The comments did not specifically address corrective actions taken or planned, dates of actions taken, and estimated completion dates of planned actions for implementing the recommendation. Therefore, to facilitate the followup tracking that is required by DoD Directive 7650.3, we request that both the Assistant Secretary of Defense and the Director, Defense Security Service, provide additional management comments by January 18, 2001. The text of the management comments is in the Management Comments section. However, a matrix attached to the Director's comments was not included in the final report because the suggested changes did not affect the results and conclusions of the audit.

Appendix A. Audit Process

Scope

Work Performed. We conducted this program audit from April 2000 through August 2000 and reviewed documentation dated from May 1989 through August 2000. To accomplish the audit objective we:

- interviewed officials and obtained documentation from the offices of the Assistant Secretary of Defense (Command, Control, Communications, and Intelligence); the Director, DSS; cognizant officials and personnel involved in the acquisition and operation of the CCMS and the DSS Enterprise System; the Air Force Program Management Office; and contractor personnel;

- reviewed available documents covering program requirements, program definition, program assessments and decision reviews, periodic reporting, and program management and oversight;

- reviewed ongoing and completed work correcting the deficiencies addressed in the General Accounting Office's October 1999 report, "Inadequate Personnel Security Investigations Pose National Security Risks;" and

- evaluated the adequacy of management controls related to CCMS and DSS information technology acquisitions.

DoD-Wide Corporate Level Government Performance and Results Act Coverage. In response to the Government Performance and Results Act, the Secretary of Defense annually establishes DoD-wide corporate level goals, subordinate performance goals, and performance measures. This report pertains to achievement of the following goal, subordinate performance goals, and performance measure:

FY 2001 DoD Corporate Level Goal 2: Prepare now for an uncertain future by pursuing a focused modernization effort that maintains U.S. qualitative superiority in key warfighting capabilities. Transform the force by exploiting the Revolution in Military Affairs, and reengineer the Department to achieve a 21st century infrastructure. **(01-DoD-2)**

- **FY 2001 Subordinate Performance Goal 2.3:** Streamline the DoD infrastructure by redesigning the Department's support structure and pursuing business practice reforms. **(01-DoD-2.3)**
- **FY 2001 Subordinate Performance Goal 2.5:** Improve DoD financial and information management. **(01-DoD-2.5)**

  Performance Measure 2.5.3: Qualitative Assessment of Reforming Information Technology Management. **(01-DoD-2.5.3)**

DoD Functional Area Reform Goals. Most major DoD functional areas have also established performance improvement reform objectives and goals. This report pertains to achievement of the following functional area objectives and goals:

Information Technology Management Functional Area.

- **Objective.** Become a mission partner.
  Goal. Serve mission information users as customers. **(ITM 2.1)**
- **Objective.** Provide services that satisfy customer information needs.
  Goal. Build architecture and performance infrastructures. **(ITM 2.1)**
  Goal. Improve information technology management tools. **(ITM-2.4)**

General Accounting Office High-Risk Area. The General Accounting Office has identified several high-risk areas in the DoD. This report provides coverage of the Information Management and Technology high-risk area.

Methodology

We conducted this program audit in accordance with auditing standards issued by the Comptroller of the United States, as implemented by the Inspector General, DoD. Accordingly, we included tests of management controls considered necessary. We did not use computer-processed information to perform this audit.

Contacts During the Audit. We visited or contacted individuals and organizations within and outside DoD. Further details are available upon request.

Management Control Program Review

DoD Directive 5010.38, "Management Control (MC) Program," August 26, 1996, and DoD Instruction 5010.40, "Management Control (MC) Program Procedures," August 28, 1996, require DoD organizations to implement a comprehensive system of management controls that provides reasonable assurance that programs are operating as intended and to evaluate the adequacy of the controls.

Scope of the Review of the Management Control Program. In accordance with DoD Directive 5000.1, "Defense Acquisition," March 15, 1996, and DoD 5000.2-R, "Mandatory Procedures for Major Defense Acquisition Programs (MDAPs) and Major Automated Information System (MAIS) Acquisition Programs," March 15, 1996, acquisition managers are to apply program cost, schedule, and performance parameters to control objectives for implementing DoD Directive 5010.38 requirements. Accordingly, we limited our review to management controls directly related to the acquisition of the CCMS and the DSS Enterprise System. We also reviewed management's self-evaluation of management controls applicable to the acquisition of DSS information technology.

Adequacy of the Management Controls. Management controls were inadequate for the acquisition of the CCMS and the DSS Enterprise System. The control problems identified in this report, as they relate to the initial system deployment, were addressed by the DSS partnership with the Air Force and the Assistant Secretary of Defense (Command, Control, Communications, and Intelligence) plan to designate the DSS Enterprise System as a Major Automated Information System. However, as reported in the DSS Federal Managers' Financial Integrity Act Annual Statement of Assurance for FYs 1999 and 2000, DSS should continue reporting personnel security investigations as a material management control weakness until all overdue security clearances requiring reinvestigation are eliminated.

Adequacy of Management's Self-Evaluation. As part of the corrective action taken in response to the General Accounting Office audit, DSS developed an inventory of management control assessable units and recognized information technology as a major management control assessable unit. Risk assessments were completed and the DSS was reviewing them to develop a plan for conducting evaluations.

Prior Coverage

During the last 5 years, the General Accounting Office issued one report on security clearance background investigations. Also, three other groups issued reports specifically addressing the CCMS and Enterprise System.

- General Accounting Office Report No. NSIAD-00-12 (OSD Case No. 1901), "Inadequate Personnel Security Investigations Pose National Security Risks," October 27, 1999
- TRW, Inc., Systems Integration Group, Final Report, "TRW's Evaluation of DSS CCMS," July 21, 1999
- Air Force/MITRE Red Team report, "Red Team Recommendations-Transition Ahead," July 14, 1999
- DSS Integrated Program Team Report, "A Near-Term Strategy to Correct Deficiencies in the Enterprise System," May 1999

Appendix B. Acquisition Guidance

The Clinger-Cohen Act of 1996, Office of Management and Budget Circulars, and DoD guidance for systems acquisitions emphasize the importance of risk management when addressing policies and procedures for system and information technology acquisitions.

Clinger-Cohen Act of 1996

The Clinger-Cohen Act of 1996 requires agencies to design and implement a process for assessing and managing the risks of information technology acquisitions to include analyzing, tracking, evaluating, and reporting on risks and results of all major information technology capital investments.

Office of Management and Budget Circulars

Circular A-109. Circular A-109, "Major Systems Acquisitions," April 1976, provides acquisition management objectives and a management structure that agencies should follow to ensure the effectiveness and efficiency of the acquisition process.

Circular A-130. Circular A-130, "Management of Federal Information Resources," February 8, 1996, requires agencies to establish management oversight mechanisms that determine whether the system continues to fulfill mission requirements and to ensure that major information systems proceed in a timely fashion towards agreed-upon milestones.

DoD Guidance

DoD Directive 5000.1. DoD Directive 5000.1, "Defense Acquisition," March 15, 1996, establishes a disciplined, yet flexible, management approach for acquiring quality products. The Directive emphasizes that rigorous internal management control systems are integral elements of effective and accountable program management and that material management control weaknesses are identified through deviations from approved system acquisition program baselines.

DoD Directive 8000.1. DoD Directive 8000.1, "Defense Information Management (IM) Program," October 27, 1992, establishes policy and assigns responsibilities for the implementation, execution, and oversight of the Defense Information Management Program. The Directive requires a disciplined life-cycle approach to manage information systems to effectively execute DoD missions.

DoD Regulation 5000.2-R. DoD Regulation 5000.2-R, "Mandatory Procedures for Major Defense Acquisition Programs (MDAPs) and Major Automated Information Systems (MAIS) Acquisition Programs," March 15, 1996, requires every system acquisition program to establish cost, schedule, and performance objectives and thresholds at system acquisition program initiation. The Regulation also requires that program managers use a management process to translate operational needs and requirements into a system solution with accountable links to program definition, structure, design, assessments and reports, and oversight decision reviews.

Appendix C. Components of the Enterprise System

The following subsections provide an overview of each component of the DSS Enterprise System.

Case Control Management System

The CCMS is the centerpiece of the overall DSS Enterprise System. As the Enterprise System's guidance and control element, the CCMS provides the means for collecting and disseminating personnel investigation data. The CCMS automated the paper-intensive, manual activities performed by the DSS Operations Centers, Baltimore, Maryland, and Columbus, Ohio. CCMS receives, stores, and acts upon personnel security requests, such as personnel security updates and requests for investigation. Investigation requests require a scope determination on whether to proceed with a field investigation. If an investigation is necessary, CCMS automatically opens a case and generates the required leads. CCMS provides personnel security analysts with the required tools to manage personnel security actions and investigations. The CCMS and the DSS Enterprise System consist of a central corporate database and an automated case workflow process that feeds information into the CCMS through several interface connections.

Files Automation and Scanning Subsystem

The Files Automation and Scanning Subsystem is the second largest element of the DSS Enterprise System and manages documents that are maintained in the DSS corporate database. Paper and microfiche documents are scanned, converted to electronic image files, and stored on magnetic drives referred to as the Files Automation and Scanning Subsystem towers. Once the documents are on the towers, DSS personnel, using CCMS and Files Automation and Scanning Subsystem applications, can access them. The Files Automation and Scanning Subsystem also provides a distribution subsystem, forms processing subsystem, and a backup subsystem. The distribution subsystem creates reports containing discrete data from the DSS corporate database and Files Automation and Scanning Subsystem image files and distributes them on several mediums: internet web sites, facsimile, paper, and computer output to microfiche. The forms processing subsystem provides forms recognition and data entry to convert paper forms to discrete data that can be stored in the corporate database.

Defense Clearance and Investigations Index System

The Defense Clearance and Investigations Index system provides a central index of clearance and investigative information originated by authorized DoD agencies. An Internet web forms version, an Internet dynamic version, and a system client-server version of the application provide the information. The Defense Clearance and Investigations Index supplies information on people, companies or events, and associated tracings to authorized agencies. These agencies include:

- United States Military (Army, Navy, Air Force, and Coast Guard)
- National Security Agency
- Defense Security Service
- Inspector General, DoD
- Defense Office of Hearings and Appeals
- Defense Logistics Agency
- Washington Headquarters Service
- Defense Intelligence Agency

Other agencies (some outside DoD) also have access to the Defense Clearance and Investigations Index system. Overall, there are approximately 2700 users of the Defense Clearance and Investigations Index system worldwide. The tracings include dossiers, aliases, national agency checks, and personal clearances. Authorized users can perform a variety of functions including query, add, delete, update, and print. In addition, users can request statistical, file demand, batch error, and the Defense Clearance and Investigations Index Disclosure Accounting System reports.

Industrial Security System

The Industrial Security System assists in monitoring DoD contractors who have access to classified information and tracks the issuance, maintenance, and management of contractor clearances. The Industrial Security System, a UNIX-based Oracle database application, uses tables within the DSS corporate database. The Industrial Security System provides industrial security representatives and others with proper access privileges to data on cleared and uncleared DoD contractor facilities. The data enable DSS to track the security clearances of Defense contractors and to measure the performance of industrial security representatives. The Industrial Security System is comprised of the Industrial Security System Central, an application with the DSS corporate database, and the Industrial Security System Field, an application residing on a desktop or notebook computer using a Microsoft Access database. Industrial security representatives fax or email facility database changes to the DSS Defense Industrial Security Clearance Office and use the Industrial Security System Central update function to make additions, changes, or deletions of the facility database in the corporate database.

Electronic Personnel Security Questionnaire System

The Electronic Personnel Security Questionnaire System simplifies the information reporting process required to conduct background investigations. The function of Electronic Personnel Security Questionnaire is to streamline the data-gathering process so that complete and accurate information is collected and validated rapidly. The Electronic Personnel Security Questionnaire System is an automated data entry and validation system designed to allow personnel and security officers to quickly and easily enter the data required. The system validates the data, prints copies of the appropriate forms, and generates export diskettes for the security officer. The Electronic Personnel Security Questionnaire was designed specifically to eliminate rejection of incomplete or inaccurate investigation requests. Features in the Electronic Personnel Security Questionnaire notify users when the information is mandatory and what the format should be. Security officers do not submit personnel information for processing until the Electronic Personnel Security Questionnaire is error free and complete.

Automated Credit Manager System

The Automated Credit Manager system uses telephone modem connections to the three commercial credit reporting agencies. The Automated Credit Manager system is used to gather credit report information, which is regularly requested as part of the security clearance investigation process, on individuals under investigation. The Automated Credit Manager system transmits credit information requests, receives return credit reports, and places the collected data into the DSS Enterprise System's corporate database for CCMS processing.

Financial Crimes Enforcement Network System

The Financial Crimes Enforcement Network system application uses the computer supporting the Automated Credit Manager system and a separate dedicated secure modem to run batch queries that conduct automated checks of Financial Crimes Enforcement Network database records. Inquiries are primarily run against the Social Security Numbers of personnel under DSS investigation, but can also be run against names, dates of birth, and partial Social Security Numbers. The Financial Crimes Enforcement Network is a Department of the Treasury organization that provides a Government-wide, multi-source intelligence and analytical network to support the DSS, law enforcement, and regulatory agencies in detection, investigation, and prosecution of financial crimes.

Field Information Management System II

The Field Information Management System II is an automated system loaded in field agents' laptop computers that provides tools to:

- Create reports of investigation
- Submit leads and other case data
- Produce summary reports of case data
- Obtain data from the Personnel Investigation Center
- Manage investigative agents' data and supporting information

The Field Information Management System II manages the electronic data link used to send and receive data from agent laptops to DSS. The system was created to support DSS regional and field offices in their efforts to process cases as DSS field agents produce them. The Field Information Management System II allows data to be transferred between field agents, field offices, regional offices, and the DSS Personnel Investigation Center located in the Operations Center, Baltimore, Maryland.

Field Information Management System - Middleware

The Field Information Management System-Middleware software application allows CCMS to be used with the Field Information Management System II to convert CCMS-generated leads into Field Information Management System II action lead sheets that can be sent to the field electronically. The Field Information Management System-Middleware also translates incoming electronically transmitted Field Information Management System II reports of investigations into a CCMS-readable format.

File Control Management System

The File Control Management System is a computer application hosted on the CCMS server that allows authorized users to request dossiers from DSS repositories. The File Control Management System also provides the mechanism for a user to input data from paper and telephone requests into its corporate database. The File Control Management System verifies authorized user rights and permissions against tables in the corporate database. When a user demands a file, the File Control Management System checks the corporate database to determine whether a file from the repository has been scanned into electronic form. When a file exists, the File Control Management System interfaces with the Files Automation and Scanning Subsystem to access data relating to the file demand. If the demanded file is not in the Files Automation and Scanning Subsystem repository, a "pick ticket" displaying all of the information that is required for a file clerk to pull the microfiche is printed in the DSS Investigative Files Branch. After the file has been scanned, the corporate database is updated and the file demand is processed. The File

Control Management System - Files Automation and Scanning Subsystem interface allows the Files Automation and Scanning Subsystem to track and monitor the progress of a file demand. User/Agency demands for file data are ultimately captured in the Disclosure Accounting System. The File Control Management System was designed to replace manually routing the paper to different personnel to process a single file demand.

Disclosure Accounting System

The Disclosure Accounting System is an automated application hosted on the CCMS server that records file release data and other disclosure information in support of the Privacy Act, the Freedom of Information Act, and personnel at the DSS. The Disclosure Accounting System is run against data as an element of the corporate database and is used by DSS to record the release to DoD and non-DoD agencies of personal information used in DSS Personnel Security Investigations and the Defense Clearance and Investigations Index. The Disclosure Accounting System records who received the information, the reason for release, the releasing DSS office, the type of information released, and the release date. The Disclosure Accounting System database is populated from information passed from the File Control Management System to the Files Automation and Scanning Subsystem and from the Files Automation and Scanning Subsystem to the Disclosure Accounting System.

Authorized File Requesters

The Authorized File Requesters is a database-centered application hosted on the CCMS server that contains a listing of authorized agencies and personnel who may request DSS investigative dossiers. The Authorized File Requesters' application can also be used to run queries to search for a particular agency using a five-digit accreditation account number.

Reject Tracking System

The Reject Tracking System is an automated computer application hosted on the CCMS server that enables DSS to track paper requests that have been rejected and returned by DSS to requesters prior to their input to the CCMS. The Reject Tracking System application generates notification letters to requesters and identifies all of the deficiencies that caused the request to be rejected. The Reject Tracking System tracks suspense dates on actions requiring followup and also allows for a query capability by Social Security Number.

User Community Management System

The User Community Management System is an automated application hosted on the CCMS server that is used to grant access permissions and user rights to personnel with a need to access the CCMS and the Enterprise System. The User Community Management System records access to the various DSS automated information systems, and applications in the corporate database.

Automated Scoping Guide System

The Automated Scoping Guide System is a database-centered application hosted on the CCMS server that provides a listing of most communities by zip code and designates which DSS field offices are responsible for investigative work in each area. The application includes remarks sections that clarify scoping responsibilities and other pertinent information about specific communities. The CCMS uses the database information to automatically scope investigations in workflow, and users can access the scoping guide from DSS local area network workstations to manipulate data.

DSS Toolbar

The DSS toolbar is a custom Graphical User Interface application that serves as a front end user entry point for accessing all of the applications connected to the DSS corporate database. The Graphical User Interface connects to the DSS-developed User Community Management System and the Commercial-off-the-Shelf Password Manager software program, both of which are resident on the corporate database servers. The Graphical User Interface requires the user to log on to the database with a controlled identification number and password.

Lead Reconciliation Tool

The Lead Reconciliation Tool is an automated application tool that reconciles the field offices' databases with the DSS corporate database. The Lead Reconciliation Tool also contains an external gateway File Transfer Protocol script that is run from a desktop workstation and a Lead Reconciliation Tool component field application. The Lead Reconciliation Tool captures pertinent DSS corporate database information at the DSS Operations Center relating to Field Information Management System II-connected field offices and compares case data and statuses with the Field Information Management System II system-generated information. The Lead Reconciliation Tool gateway connects to the Field Information Management System II system and processes pending and closed Lead Reconciliation Tool data and File Transfer Protocol's consolidated packages of information via a DSS Link connection to each DSS field office operational location. DSS field offices perform data reconciliation, case management, and statistical reporting functions using the field component of the Lead Reconciliation Tool application.

Internal File Transfer Protocol Server

The DSS Internal File Transfer Protocol Server is a stand-alone, DSS Intranet-connected computer available inside the DSS firewalls for DSS local area network File Transfer Protocol use. Several of the DSS Enterprise System applications use File Transfer Protocol to transfer and handle data files. At DSS, File Transfer Protocol actions are accomplished with manual and automated connections. File Transfer Protocol is a standard protocol that is the simplest way to exchange files between connected computers.

External File Transfer Protocol Server

The DSS External File Transfer Protocol Server is a stand-alone, DSS Internet-connected computer available outside the DSS firewalls for external File Transfer Protocol use. File Transfer Protocol is a standard protocol that is the simplest way to exchange files between computers connected on the Internet. At DSS, File Transfer Protocol actions are accomplished with manual and automated connections.

External Office of Personnel Management Gateway

The external Office of Personnel Management gateway is hosted on a computer at DSS that provides a dedicated communications link supporting data exchange between the DSS Defense Clearance and Investigations Index and the Office of Personnel Management's Security Suitability Investigations Index. Although housed on a separate computer, the gateway is an essential part of the Defense Clearance and Investigations Index and the Security Suitability Investigations Index applications.

External Immigration and Naturalization Service Gateway

The external Immigration and Naturalization Service gateway is hosted on a computer at DSS that provides a dedicated communications link supporting data exchange between the Immigration and Naturalization Service master index and the DSS corporate database. Immigration and Naturalization Service files contain the location of naturalization certificates, citizenship certificates, visas, records of aliens, and other information that is checked as part of the national agency check process when conducting security investigations. The gateway also supports data exchange for Financial Crimes Enforcement Network information obtained by DSS as a liaison on behalf of the Immigration and Naturalization Service.

External Interface to the Central Intelligence Agency

The External Interface to the Central Intelligence Agency is a batch computer application process that involves operator-assisted manual actions and automated computer actions. The application processes file demands created through the Defense Clearance and Investigations Index or the File Control Management System and their related application sub-processes. The Central Intelligence Agency External Interface application results in the creation and reading of a data tape that is either sent to the Central Intelligence Agency or received from the Central Intelligence Agency for processing.

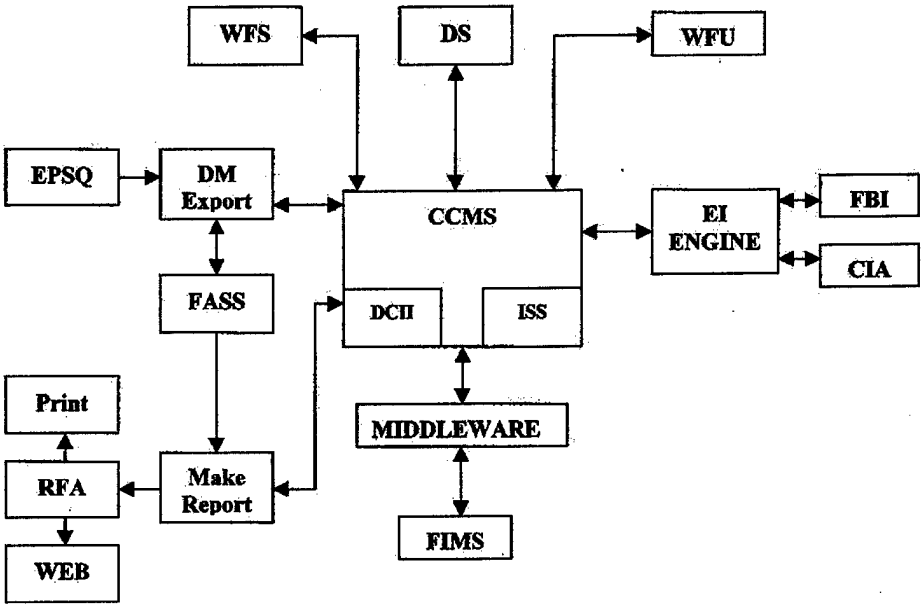
External Interface to the Federal Bureau of Investigation

The External Interface to the Federal Bureau of Investigation is a batch computer application process that involves operator-assisted manual actions and automated computer actions. The Federal Bureau of Investigation conducts three types of checks for DSS as part of the personnel investigation process. Requests for information come from CCMS leads that generate Federal Bureau of Investigation identification fingerprint card check, name check, and combined name and fingerprint card check requests. The Federal Bureau of Investigation External Interface application results in the creation and reading of a data tape that is either sent to the Federal Bureau of Investigation or received from the Federal Bureau of Investigation for processing.

Navy Joint Adjudication and Clearance System

The Navy Joint Adjudication and Clearance System is hosted on the CCMS and Enterprise System server and, in conjunction with the DSS corporate database, contains personnel security data on all Department of the Navy and Marine Corps military and civilian personnel and Coast Guard military personnel. The Navy Joint Adjudication and Clearance System also serves as an internal case management system that supports the day-to-day operations of the Navy's central adjudication facility. Message traffic generated by the system informs recipient commands on the status of security clearance requests or final results of personnel security determinations. Additionally, the Navy Joint Adjudication and Clearance System provides data management and analysis reports, audit trails, and historical case-tracking information.

Appendix D. Enterprise System High Level Process View



LEGEND	
CIA	Central Intelligence Agency
CCMS	Case Control Management System
DCII	Defense Clearance and Investigations Index
DM	Document Management
DS	Device Server
EI	External Interface
EPSQ	Electronic Personnel Security Questionnaire
FASS	Files Automation and Scanning Subsystem
FBI	Federal Bureau of Investigation
FIMS	Field Information Management System
ISS	Industrial Security System
RFA	Report for Adjudication
WFS	Workflow Server
WFU	Workflow User

Appendix E. Status of TRW Inc., Recommendations by Priority Ranking

Priority	TRW Recommendations	Status
1.	Establish and operate a program management office organization	Complete
2.	Manage CCMS recover and sustainment	Complete
3.	Manage replacement systems acquisition	In-Progress
4.	Institute formal flow control of the CCMS Workflow tool	In-Progress
5.	Develop a more appropriate year 2000 test environment	Complete
6.	Upgrade infrastructure baseline	In-Progress
7.	Upgrade and/or replace workflow product	In-Progress
8.	Develop concept of operations and requirements specification documents	In-Progress
9.	Eliminate the use of "route-back" within CCMS workflows	In-Progress
10.	Establish an integrated DSS Enterprise Systemwide action team	Complete
11.	Develop a high level workflow performance model	In-Progress
12.	Establish a replacement system acquisition strategy	In-Progress
13.	Investigate upgrading the database management system	In-Progress
14.	Use contractor facilities for year 2000 testing	Complete
15.	Evaluate the utility of manually archiving data	In-Progress
16.	Analyze and optimize CCMS/Files Automation and Scanning Subsystem configuration to reduce instability	In-Progress
17.	Evaluate rebalancing workload on Digital Equipment Corporation 8400 computers and Oracle databases	In-Progress
18.	Evaluate other methods to reduce CCMS/Files Automation and Scanning Subsystem instability	Contingent[1]
19.	Develop a more robust CCMS/Files Automation and Scanning Subsystem interface	In-Progress
20.	Reduce number of overhead functions associated with each workflow task	In-Progress

[1]Implementation depends on results of another TRW recommendation.

Priority	TRW Recommendations	Status
21.	Correct errors in request-for-adjudication processing	In-Progress
22.	Implement general hardware recommendations	In-Progress
23.	Upgrade microfiche scanning processes to increase reliability	In-Progress
24.	Evaluate additional Document Management Export debugging strategies	Contingent[1]
25.	Enhance Document Management Export error recovery	In-Progress
26.	Investigate the effect of more powerful central processing units	Complete
27.	Improve the paper-based request for adjudication process	In-Progress
28.	Evaluate and expedite fixes for current known data integrity problems	In-Progress
29.	Implement database configuration changes to optimize performance	In-Progress
30.	Analyze performance requirements for system improvements	In-Progress
31.	Identify and collect performance metrics	In-Progress
32.	Implement backup and restore capability	Pending[2]
33.	Investigate electronic dissemination of requests for adjudication	Complete
34.	Implement percentage of items awaiting operator action as basis for workflow performance	In-Progress
35.	Implement improved manual case entry process	Complete
36.	Perform routine backups of databases, mailboxes, queues, relevant directories and files	Pending[2]
37.	Plan for long-term system maintenance	In-Progress

[1]Implementation depends on results of another TRW recommendation.
[2]Action will be resourced when funding becomes available.

Appendix F. Report Distribution

Office of the Secretary of Defense

Under Secretary of Defense (Comptroller/Chief Financial Officer)
  Deputy Chief Financial Officer
  Deputy Comptroller (Program/Budget)
Assistant Secretary of Defense (Command, Control, Communications, and Intelligence)
  Deputy Assistant Secretary of Defense (Security and Information Operations)
  Director, Information Technology Acquisition and Investments

Department of the Army

Auditor General, Department of the Army

Department of the Navy

Naval Inspector General
Auditor General, Department of the Navy

Department of the Air Force

Assistant Secretary of the Air Force (Financial Management and Comptroller)
Auditor General, Department of the Air Force

Other Defense Organizations

Director, Defense Security Service
  Inspector General, Defense Security Service
Director, Defense Contract Audit Agency
Director, Defense Contract Management Agency
Director, Defense Logistics Agency
Director, National Security Agency
  Inspector General, National Security Agency
Inspector General, Defense Intelligence Agency

Non-Defense Federal Organization

Office of Management and Budget

Congressional Committees and Subcommittees, Chairman and Ranking Minority Member

Senate Committee on Appropriations
Senate Subcommittee on Defense, Committee on Appropriations
Senate Committee on Armed Services
Senate Committee on Governmental Affairs
House Committee on Appropriations
House Subcommittee on Defense, Committee on Appropriations
House Committee on Armed Services
House Committee on Government Reform
House Subcommittee on Government Management, Information, and Technology, Committee on Government Reform
House Subcommittee on National Security, Veterans Affairs, and International Relations, Committee on Government Reform

This page was left out of original document

Assistant Secretary of Defense (Command, Control, Communications, and Intelligence) Comments

ASSISTANT SECRETARY OF DEFENSE
6000 DEFENSE PENTAGON
WASHINGTON, DC 20301-6000

COMMAND, CONTROL, COMMUNICATIONS, AND INTELLIGENCE

December 8, 2000

MEMORANDUM FOR OFFICE OF ASSISTANT INSPECTOR GENERAL FOR AUDIT,
ATTN: DIRECTOR, ACQUISITION MANAGEMENT

SUBJECT: Audit Report on Program Management of the Defense Security Service Case Control Management System (Project No. D2000AL-0159

This is in response your memorandum of September 29, 2000, regarding the draft Defense Security Service (DSS) Case Control Management System (CCMS) audit report.

We concur with your findings and recommendation. DSS and the Air Force have made a great deal of progress in restoring system acquisition discipline to CCMS. We stand committed to seeing that this continues in the future. Our intent is to designate CCMS/Enterprise System (target architecture) as an ACAT IAC program with the Air Force (LtGen Leslie Kenne) as the milestone decision authority. As an ACAT IAC program, the Air Force will be required to submit DAES quarterly reports, and obtain Clinger-Cohen Act certification from C3I for CCMS/Enterprise System prior to each milestone approval.

If you have any questions or require further information regarding our efforts on CCMS, please contact Ray Boyd, my action officer in the Investment and Acquisition Directorate, at (703) 602-0980, ext. 180.

Arthur L. Money

Defense Security Service Comments

DEFENSE SECURITY SERVICE
1340 BRADDOCK PLACE
ALEXANDRIA, VA 22314-1651

NOV 2 9 2000

Reply to
Attn of: OIG

SUBJECT: Draft of a Proposed Department of Defense Inspector General Audit Report, "Program Management of the Defense Security Service Case Control Management System" (Project No. D2000AL-0159)

THRU: Delores I. Moeller
Deputy Director for Resources

TO: Thomas F. Gimble, Director
Acquisition Management Directorate, DoDIG

1. The Defense Security Service (DSS) concurs with the finding and recommendation as stated in the DoDIG report. After careful analysis, the DSS Enterprise System is determined to be the best solution for the near term. Oversight of the development and migration to the target architecture should be accomplished through a joint Office of the Assistant Secretary of Defense (OASD) (C3I)/DSS modified ACAT 1C program, including a semiannual TRW process review, a quarterly presentation to the DSS Technical Advisory Committee, and weekly/monthly reporting by Air Force Program Management Office to the Defense Acquisition Council at the Air Force Electronic Systems Command, OASD (C3I), and DSS.

2. We recommend a few minor additions/changes (see attached table). First column indicates the page and paragraph number; the second contains the paragraph title (where appropriate); third contains our comments; and last contains a rationale (when necessary for clarification). *

3. We appreciate the opportunity to review and comment on this report. For additional information on our comments, please contact Ms. Ann Johnson at (410) 865-2631 (ann.johnson@mail.dss.mil).

CHARLES J. CUNNINGHAM JR.
Director

Attachment

*Appropriate corrections were made to the final report. (Table not included in this report)

Audit Team Members

The Acquisition Management Directorate, Office of the Assistant Inspector General for Auditing, DoD, prepared this report.

Thomas F. Gimble
Mary Lu Ugone
Charles M. Santoni
David M. Wyte
Steven J. Bressi
Donald Stockton
Robert R. Johnson
Walter S. Bohinski

December 1, 2000

Honorable Richard K. Armey
Majority Leader
House of Representatives
Washington, D.C. 20515-6503

Dear Congressman Armey:

This is in reply to the joint letter of October 12, 2000, from the Chairmen of the Senate Committee on the Budget and Committee on Governmental Affairs, the House Government Reform Committee, House Budget Committee and you on Department of Defense (DoD) management challenges. The joint letter requested that we update our previous assessments of the most significant management problems facing the DoD; identify related reports and recommendations; comment on progress being made in resolving significant problems; and identify programs that have had questionable success in achieving results.

The size and diversity of DoD operations makes it difficult to summarize the vast array of management challenges confronting the Department and to determine those of most significance. There are several hundred ongoing management initiatives to address challenges visible at the Office of the Secretary of Defense level and many more being carried out within the Military Departments, Defense Agencies, Joint Staff and Combatant Commands. Similarly, the Department performs a huge number of self-assessments, including well over 200 audit and evaluation reports with about 1,000 recommendations annually from this office. The General Accounting Office also reports extensively on DoD matters. Nevertheless, there are troubling gaps in audit coverage in many areas of the Department, which are caused primarily by resource constraints. Therefore we caution that the limited number of reports and recommendations related to some management problem areas, such as Health Care and Readiness, are not indicative of the actual scope of the challenges in those areas. Despite the lack of comprehensive audit coverage in certain areas, we feel confident in identifying the following principal management challenges:

1. Information Technology Management

2. Information System Security

3. Other Security Concerns

4. Financial Management

5. Acquisition

6. Health Care

7. Supply Inventory Management

8. Other Infrastructure Issues

9. Readiness

10. Human Capital

These 10 challenges are essentially the same as those we identified last year, except that Turbulence from Change has been broadened to Human Capital. The detailed information that you requested on each area and on poorly performing programs is enclosed. If there are questions, please contact me or Mr. John R. Crane, Director, Office of Congressional Liaison, at (703) 604-8324.

Sincerely,

(signed)

Donald Mancuso
Acting Inspector General

Enclosure

Detailed Response to Congressional
Request of October 12, 2000,
on DoD Management Challenges

Information Technology Management

The Challenge. The DoD has succeeded in developing the concept of the Global Information Grid, fielding certain key systems like the Global Command and Control System, overcoming the formidable Y2K conversion problem and eliminating redundant in-house data processing capacity. With respect to improving risk management across the board in information system acquisitions, however, it is difficult to see substantive improvement. The separate and ineffective information systems acquisition rules were merged with the standard DoD weapon systems acquisition guidelines and new information system oversight procedures are being implemented, but are unproven. The Department has compiled the central registry of systems required by Section 8121 of the Defense Appropriations Act for FY 2000 and has made the initial Clinger-Cohen Act compliance certifications required under Section 8121 for major systems at acquisition milestones. The IG, DoD, will issue a series of reports over the next several months on the effectiveness of the certification process, which probably will require further refinements. Meanwhile, virtually every audit of a DoD information technology acquisition project indicates serious flaws.

The DoD command, control, intelligence and business functions depend heavily on network based information technologies. This dependence is not bad in itself, since these technologies have enabled dramatic increases in efficiency and capability, but the vulnerabilities created by this dependence must be addressed. In addition to ensuring that new systems are sufficiently capable, secure and interoperable, the DoD must focus over the next several years on the growing problems created by under investment in information technology infrastructure, increased competition for use of the radio frequency spectrum, and severe recruiting, retention and skills maintenance problems in the DoD information technology workforce. We are putting considerable emphasis on audit coverage of the DoD information technology area, including the new Navy/Marine Corps Intranet experiment in adopting seat management on a massive scale, but the fact that DoD has many thousand essential systems and projects makes comprehensive audit coverage infeasible.

Most Significant Recent Reports on Information Technology

D-2000-57, Summary of DoD Year 2000 Computing Issues IV, 12/16/99

D-2000-63, Information Technology Funding in the Department of Defense, 12/17/99

D-2000-125, Reporting Requirements for Major Automated Information System programs, 5/17/00

D-2000-142, Defense Information Systems Agency's Acquisition Management of the Global Combat Support System, 6/9/00

D-2000-151, Acquisition and Management of the Defense Joint Accounting System, 6/16/00

D-2000-162, Summary of Audits of Acquisition of Information Technology, 7/13/00

Open Recommendations. The most significant open IG, DoD, recommendations on Information Technology Management are as follows:

1. Because the DoD had never conducted a proper acquisition milestone review for the Defense Joint Accounting System (DJAS), we recommended that the Assistant Secretary of Defense (Command, Control, Communications and Intelligence) not approve DJAS for use until the Defense Finance and Accounting Service has demonstrated that the current acquisition strategy will reduce risks, ensure the required functionality for users, and meet DoD acquisition standards and Clinger-Cohen Act requirements. (Report D-2000-151, 6/16/00)

2. To enable senior managers to provide effective oversight, we recommended that the Assistant Secretary of Defense (Command, Control, Communications and Intelligence) implement procedures to verify project status information in Defense Acquisition Executive Summary reports and make full use of those reports to monitor the progress of selected systems. (Report D-2000-125, 5/17/00).

3. To address the serious operational problems created by conflicting requirements for use of the radio frequency spectrum, we recommended that DoD improve coordination with nations hosting U.S. forces; implement centralized management of international telecommunications; and revise system acquisition guidance to identify potential deployment constraints. (Report 99-009, 10/9/98)

4. To achieve better implementation of the DoD Joint Technical Architecture for information technology systems, we recommended that a detailed methodology be developed for cross-organizational and cross-functional coordination of implementation plans. (Report 98-023, 11/18/97)

5. To improve interoperability, we recommended standardizing the message reporting formats for tactical intelligence dissemination. (Report 95-292, 8/17/95)

Closed Recommendations. The most significant recommendations that were recently closed in this area are as follows:

1. To correct problems with controlling sensitive case evidence, the Armed Forces Institute of Pathology implemented a new management information system. (Report 99-199, 4/2/99)

2. To enable better accountability, the White House Communications Agency performed a complete inventory of its telecommunications assets. (Report 96-33, 11/29/95)

3. To avoid Year 2000 conversion problems, the DoD implemented numerous audit recommendations, some of which were closed during the late stages of the conversion period. The official conversion period ended on March 31, 2000. For example, measures to avoid selling or donating non-Y2K compliant biomedical devices were fully implemented and documented toward the end of 1999 and non-compliant items in medical war reserves were identified as recently as early 2000. All Y2K-related actions are now closed. (Multiple reports)

4. To avoid restrictions on training and potential operational problems, the DoD and the Republic of Korea established agreements to avoid frequency spectrum conflicts affecting Army air defense weapons. (Report 98-211, 9/24/98)

Information System Security

The Challenge. Our semiannual report to the Congress for the semiannual period ending March 31, 2000, discussed the growing threat to DoD, other government, and commercial information networks from criminals, vandals, hostile states and terrorists. We reported that, while much effort was being made, the Federal and DoD responses remained disjointed. As of late 2000, there are still numerous policy gaps and much work remains to develop effective coordination mechanisms, especially for national infrastructure protection. The DoD has a robust intrusion detection and reaction capability in place, but most other aspects of the Defense Information Assurance Program are still being developed. Although it was widely assumed that the knowledge and experience gained in the Y2K conversion would be applied to the information security area, there are few signs that has happened.

Most Significant Recent Reports on Information System Security

D-2000-058, Identification and Authentication Policy, 12/20/99

D-2000-122, Information Assurance in the Advanced Logistics Program, 5/12/00

D-2000-124, Information Assurance Challenges: A Summary of Audit Results Reported December 1, 1998, through March 31, 2000, 5/15/00

D-2000-130, Foreign National Access to Automated Information Systems, 5/26/00

D-2001-013, DoD Compliance With the Information Assurance Vulnerability Alert Policy, 12/1/00

Open Recommendations. The most significant open IG, DoD, recommendations related to Information System Security are as follows:

1. To achieve better results from the December 1999 DoD initiative to establish an Information Assurance Vulnerability Alert process, we recommended that the Assistant Secretary of Defense (Command, Control, Communications and Intelligence) issue formal guidance and a detailed implementation plan. We also recommended that certain DoD components, which had not registered in the program database or reported in accordance with DoD direction, take corrective action to ensure consistent and full implementation of the plan. (Report D-2001-013, 12/1/00)

2. To improve controls over access by foreign nationals to DoD information systems and networks in settings such as joint international program offices, we recommended that the Army and Navy revise their regulations related to access to local area networks and other information media. (Report D-2000-130, 5/26/00)

3. To provide more consistency in the Defense Information Assurance Program, we recommended that the Assistant Secretary of Defense (Command, Control, Communications and Intelligence) update, clarify and standardize policy to define security requirements, especially those pertaining to identification and authentication. (Report D-2000-058, 12/20/99)

Closed Recommendations. The most significant of our recently closed recommendations in this area are as follows.

1. To address information assurance vulnerabilities, computer security measures such as defining, controlling and monitoring user access to the Defense Joint Military Pay System were implemented. (Report 96-175, 6/15/00)

2. To improve security, a variety of recommended actions were taken to address vulnerabilities related to the Defense Civilian Pay System. (Reports 99-107, 3/16/99 and 99-128, 6/29/99)

3. To improve security, controls were strengthened for the Defense Property Accountability System. (Report 99-225, 7/29/99)

4. To improve security, a number of recommended controls were implemented for the Standard Automated Materiel System. (Report D-2000-96, 3/7/00)

Other Security Concerns

The Challenge. Although the threats posed by unauthorized intrusions into DoD information systems have received considerable and justifiable attention, a wide range of other security threats confront the DoD. Those threats include terrorism against U.S. personnel and facilities, conducted by either conventional or non-conventional means, and the disclosure or theft of sensitive military technology. The recent terrorist attack on the U.S.S. Cole in Yemen and security breaches at the Department of Energy, the Central Intelligence Agency and DoD graphically demonstrated that security vulnerabilities need to be matters of utmost concern.

Recent audits have indicated that the DoD needs to improve security measures to guard against both internal and external threats. We have not audited force protection issues, but we have extensively reviewed a number of other areas where unacceptable vulnerability exists. These include the Defense Personnel Security Program, which in 1999 was failing badly and allowing hundreds of thousands of overdue security clearance requests to accumulate. The Department took aggressive measures during 2000 to address the problems at the Defense Security Service and the situation has somewhat stabilized. However, much remains to be done to correct past problems and attain a fully effective security clearance program for DoD and contractor personnel. For example, the DoD still lacks a prioritization process for personnel security investigations.

Similarly, there is a consensus in the Executive Branch and Congress that the export license regime of the 1990's was inefficient and probably ineffective in controlling the unintended loss of U.S. military technology. During 2000, the DoD worked with other Federal agencies to streamline the licensing processes and approved additional resources to improve the speed and value of license application reviews. The task of determining to what extent the fundamental national export control policies need to change, however, remains unfinished business for the next Administration and Congress.

It is important to view security as a paramount consideration for virtually all DoD programs and operations. Issues such as properly demilitarizing military equipment before disposal, ensuring that computers being sold or transferred outside the DoD contain no classified material, and controlling the access of contractors and visitors to technical information at military engineering organizations and laboratories all need more attention. We are focusing on those issues in ongoing audit and follow-up efforts.

Most Significant Recent Reports and Testimony on Other Security Concerns

Testimony to the Senate Armed Services Committee on National Security Implications of Export Controls and the Export Administration Act of 1999, 3/23/00

D-2000-110, Export Licensing at DoD Research Facilities, 3/24/00

D-2000-111, Security Clearance Investigative Priorities, 4/5/00

Testimony to the Senate Armed Services Committee on Issues Facing the Department of Defense Regarding Personnel Security Clearance Investigations, 4/6/00

Testimony to the Senate Committee on Governmental Affairs on Export Control Implementation issues, 5/26/00

D-2000-134, Tracking Security Clearance Requests, 5/30/00

Report on Allegations of Breaches of Security: Dr. John M. Deutch, 8/28/00

Testimony to the Subcommittee on National Security, Veterans Affairs and International Relations, House Committee on Government Reform, on Defense Security Service Oversight, 9/20/00

D-2001-007, Foreign National Security Controls at DoD Research Laboratories, 10/27/00

D-2001-008, Resources of DoD Adjudication Facilities, 10/30/00

Open Recommendations. The most significant open IG, DoD, recommendations in the area of security matters, other than those issues covered under Information System Security, are as follows:

1. To ensure that the continuing problem of delayed personnel security clearances and clearance updates is not aggravated by insufficient capacity for adjudicating investigative results, we recommended that the Directors and Chiefs of the DoD eight central adjudication facilities determine the resources required, considering all factors that affect the adjudication and appeals processes. We recommended that the Secretaries of the Army, Navy, and Air Force; the Chairman of the Joint Chiefs of Staff; and the Directors of the Defense Intelligence Agency, the Defense Office of Hearings and Appeals, the National Security Agency, and the Washington Headquarters Services provide sufficient resources to adjudicate and process appeals. We recommended that the Assistant Secretary of Defense (Command, Control,

Communications and Intelligence), in conjunction with the eight central adjudication facilities, analyze the impact on workload of the initial fielding of the Joint Personnel Adjudication System. Finally, we recommended that the Under Secretary of Defense (Comptroller) and the Assistant Secretary of Defense (Command, Control, Communications and Intelligence) review the DoD Components' budget submissions to ensure that the DoD budget for FY 2002 and the outyears enables the central adjudication facilities to meet forecasted workload requirements. (Report D-2001-008, 10/30/00)

2. To tighten controls over the release of technical information to foreign visitors to DoD laboratories, we recommended that the Director, Defense Advanced Research Projects Agency, and the Department of the Navy ensure foreign disclosure instructions from foreign visit approval authorities are disseminated to the program managers hosting foreign nationals. We recommended that the Director, Defense Advanced Research Projects Agency, enforce and improve security procedures to ensure visits by foreign nationals are sufficiently documented. We also recommended that the Director, Defense Advanced Research Projects Agency, prepare a manual providing specific procedures for the preparation of Visit Control Center records and ensure the Defense Intelligence Agency visit approval letter is used as the primary source document for information regarding official foreign national visitors. (Report D-2001-007, 10/27/00)

3. To preclude disclosure of sensitive information, we recommended that the hard drives of computers being transferred to non-DoD users or sold be destroyed. (Report of Investigation on Dr. John M. Deutch, 8/28/00)

4. To eliminate the inefficiencies created by the inability of the Defense Security Service (DSS) to track all personnel security requests and provide feedback on their status to requestors during the investigative process, we recommended that DSS take measures to acquire the requisite tracking capability. (Report D-2000-134, 5/30/00)

5. To improve the efficiency of the DoD personnel security clearance investigative efforts, we recommended that the Assistant Secretary of Defense (Command, Control, Communications and Intelligence) implement a process for prioritizing security clearance requests. (Report D-2000-111, 4/5/00)

6. To achieve better compliance with Federal export control regulations requiring "deemed export" licenses for technical information released by DoD to foreign governments, firms or individuals, we recommended that the Under Secretary of Defense for Policy coordinate with the Departments of Commerce and State to develop guidance for applying Federal deemed export licensing requirements and require implementation of that guidance by the Military Departments. In addition, we recommended that the Director, Defense Research and Engineering, coordinate with the Departments of Commerce and State to develop guidance for applying deemed export licensing requirements at DoD research facilities and develop export control procedures to guide DoD research facilities with regard to foreign national visits. We also recommended that the Deputy Under Secretary of Defense (International and Commercial Programs) update DoD instructions to give the Military Departments direct coordination authority with the Department of Commerce for all data exchange agreement annexes. Further, we recommended that the Military Departments update existing guidance to require coordination of data exchange agreement annexes with the Department of Commerce. (Report D-2000-110, 3/24/00)

7. To eliminate several deficiencies, we recommended improvements in guidance, training and data bases related to the export license review process. (Report 99-186, 6/18/99)

8. To achieve better efficiency and enhance confidence in the consistency and competence of decisions made on personnel security clearance investigative results, we recommended implementing a peer review program between adjudication facilities and implementing a professional training certification program for adjudicators. (Report 98-124, 4/27/98)

9. To achieve more efficient, effective and secure practices for handling and disposing of Defense material in the possession of contractors, we recommended changing regulations to require identification of munitions list items early in the acquisition process. (Report 97-134, 4/22/97)

Closed Recommendations. The most significant of our recommendations that were recently closed in this area are as follows:

1. To assure the quality of adjudication of personnel security clearance investigation results, we recommended developing standard training and the Department has done so. The

portion of this recommendation related to certification remains open, however, as indicated in Item 8 above. (Report 98-124, 4/27/98)

2. To avoid unnecessary investigations and administrative delays, the DoD changed policy to assure reciprocity among DoD special access programs. (Report 98-67, 2/10/98)

Financial Management

The Challenge. The DoD remains unable to comply with the requirements in the Chief Financial Officers Act of 1990 and related legislation for auditable annual financial statements. The results of audits of the DoD-wide and other major financial statements for FY 1999 were essentially the same as in previous years. The Military Retirement Fund statements received a clean audit opinion, but all other DoD financial statements were unauditable. Previous DoD goals for obtaining clean opinions on all or most annual statements during the FY 2000 to FY 2003 timeframe were unrealistic and it is unclear what a realistic goal would be at this point. A few relatively small DoD organizations and funds may achieve favorable opinions in the near future, but the major funds still pose a formidable challenge. The Department also has major concerns that the Federal Accounting Standards Advisory Board could issue guidance that would seriously complicate this challenge.

During the past year, the DoD made reasonable progress in addressing major impediments to favorable audit opinions. Policies were issued to implement various new Federal accounting standards and contractors were engaged to provide their expertise on a variety of issues, such as determining the value of different categories of property. In addition, the Department took steps to apply the lessons learned from the successful DoD Y2K conversion program to the financial system compliance effort. The DoD Senior Financial Management Council, which had not met for several years, was reconstituted to ensure senior management involvement and coordination. The initial milestone to identify the critical systems for financial reporting, March 2000, was unattainable and efforts to define criticality and identify systems continue, but we strongly support this initiative.

The IG, DoD, General Accounting Office (GAO) and Military Department auditors are developing a standard audit approach for validating the progress of the critical systems toward full compliance. Resources permitting, we will seek to provide the same kind of strong support that helped the Y2K conversion to succeed, but the system remediation and validation workload will require considerable contractor support to the components, including the Defense Finance and Accounting Service.

One of the benefits of using the Y2K management approach for financial systems compliance is that it provides good metrics for that particular aspect of the DoD financial management improvement effort. As welcome as those metrics will be for measuring system compliance status, however, they will not measure the financial usefulness of the data to managers and appropriators. Numerous recent statements and testimony to Congress by the Office of Management and Budget (OMB), GAO

and DoD officials have stressed that the ultimate goal of financial management reform legislation is ensuring useful financial information for sound decision-making, not merely clean audit opinions on annual financial statements. We strongly agree. Audit opinions are a simple and readily understandable metric, but judging the usefulness of financial information is far more difficult. Likewise, audit opinions on financial statements provide little insight into the efficiency of functions such as paying contractors or capturing the cost of operations of individual bases and work units. The DoD has long-standing deficiencies in both of those areas.

Most Significant Recent Reports and Testimony on Financial Management

D-2000-69, Department of Defense Agency-Wide Statement of Budgetary Resources, 12/29/99

D-2000-91, Internal Controls and Compliance with Laws and Regulations for the DoD Agency-Wide Financial Statements for FY 1999, 2/25/00

Testimony to the Subcommittee on Government Management, Information and Technology, House Government Reform Committee, on Defense Financial Management, 5/9/00

D-2000-136, Reporting of Performance Measures in the DoD Agency-Wide Financial Statements, 5/31/00

D-2000-139, Controls Over the Integrated Accounts Payable System, 6/5/00

D-2000-156, DoD Payroll Withholding Data for FY 1999, 6/29/00

Testimony to the Task Force on Defense and International Relations, House Budget Committee, on Department of Defense Financial Management, 7/20/00

D-2000-168, Data Supporting the Environmental Liability Line Item on the FY 1999 DoD Financial Statements, 7/27/00

D-2000-172, Accuracy of the FY 1999 Additions, Deletions and Modifications to the Military Departments' Real Property Databases, 8/11/00

D-2000-179, Department-Level Accounting Entries for FY 1999, 8/18/00

D-2000-194, Demographic Data Supporting the DoD Military Retirement Health Benefits Liability Estimate, 9/29/00

Open Recommendations. The most significant open IG, DoD, recommendations related to Financial Management are as follows:

1. To decrease the volume of accounting adjustments made in compiling DoD financial statements and to eliminate unsupported adjustments, we recommended that the Under Secretary of Defense (Comptroller) develop a set of corrective measures as part of the DoD Chief Financial Officers Act Implementation Strategies. (Report D-2000-179, 8/18/00)

2. To improve the accuracy of the estimates included in DoD financial statements for environmental cleanup and hazardous waste disposal liabilities, we recommended that the Deputy Under Secretary of Defense (Environmental Security) revise applicable guidance. (Report D-2000-168, 7/27/00)

3. To ensure better accuracy in withholding required amounts from DoD civilian payrolls, we recommended that the personnel and financial management communities ensure accurate payroll election records and prompt transmission of personnel payroll data; correct errors found by auditors; implement a review system for employee payroll elections; and establish performance measures for assessing the accuracy of payroll withholding data. We also recommended that the Director, Defense Finance and Accounting Service, develop software capable of correctly extracting electronic files that support the withholding amounts reported and implement management control procedures to ensure clear identification and communication of responsibilities. (Report D-2000-156, 6/29/00)

4. To improve the linkage between DoD Government Performance and Results Act reporting and annual financial statements, we recommended that the Under Secretary of Defense (Comptroller) develop consistent program categories, performance goals, and measures; modify the DoD Financial Management Regulation to instruct preparers of the Statements of Net Cost to use program cost elements consistent with performance goals; address requirements for managerial cost accounting systems capable of supporting performance measurement efforts in future versions of the DoD Financial Management Improvement Plan; and include a discussion of performance measures in the Overview section of future DoD Agency-wide financial statements. (Report D-2000-136, 5/31/00)

5. To reduce the volume of disbursements that are not matched to obligation records, we recommended that the Under Secretary of Defense (Comptroller) revise policy to set strict time standards for resolving problem in-transit disbursements. (Report 99-135, 7/20/99)

6. To achieve necessary financial control, we recommended a complete reconciliation of the National Guard and Reserve Equipment Appropriation by the National Guard Bureau, which subsequently transferred its accounting function to the Defense Finance and Accounting Service. (Report 99-087, 2/24/99)

7. To reduce the possibility of an Antideficiency Act violation and comply with DoD policy, we recommended that the National Guard Bureau establish administrative obligations for overage unmatched disbursements in its Army accounts. (Report 98-30, 12/3/97)

8. To facilitate accurate billing for U.S. military expenses that will be reimbursed by the United Nations, we recommended Under Secretary of Defense (Comptroller) actions to define the cost elements to be considered and revise regulations accordingly. (Report 97-77, 1/27/97)

9. To improve the accuracy of Navy accounting data, we recommended that performance measures be established to track compliance with policy to record obligations within 10 days. (Report 96-145, 6/6/97)

10. To improve financial control of DoD contracts, we recommended that the Defense Finance and Accounting Service make a concerted effort to reduce the backlog of unreconciled contracts to the equivalent of six-months work at Columbus Center. (Report 96-141, 6/4/96)

11. To eliminate incorrectly distributed Combined Federal Campaign deductions, we recommended that the Defense Finance and Accounting Service make procedural and payroll system changes. (Report 95-244, 6/21/95)

12. To ensure accurate billing to Foreign Military Sales Customers, we recommended that the Under Secretary of Defense (Comptroller) revise regulations on how to calculate packing, crating and handling costs. (Report 91-055, 2/27/91)

Closed Recommendations. The most significant of our recommendations in this area that were recently closed are as follows:

1. To apply lessons learned from the successful DoD Year 2000 Conversion to the challenge of improving the nearly 200 information systems used to compile DoD financial statements, DoD has adopted essentially the same management approach. (Report D-2000-41, 11/26/99)

2. To improve financial reporting related to DoD real property, the Chief Financial Officer revised regulations to specify what supporting documentation must be retained to validate the cost of acquiring, constructing or improving that category of assets. (Report 99-243, 8/27/99)

3. To improve internal controls, the Defense Finance and Accounting Service issued written guidance for journal voucher entries on financial records. (Report 98-50, 1/20/98)

4. To improve the reliability of contingency liability amounts shown on DoD financial statements, DoD issued guidance requiring the verification, validation and accreditation of computer models used to compute "cost to complete" estimates for the Defense Environmental Restoration Program. (Report 99-209, 7/9/99)

Acquisition

The Challenge. The DoD is working toward the goal of becoming a world-class buyer of best value goods and services from a globally competitive industrial base. The Department hopes to achieve this transformation through rapid insertion of commercial practices and technology, business process improvement, creating a workforce that is continuously retrained to operate in new environments, and heavily emphasizing faster delivery of material and services to users. In order to fulfill these objectives, the DoD has initiated an unprecedented number of major improvement efforts, including at least 40 significant acquisition reform initiatives.

Despite the previous successes and continued promise of reforms, the business of creating and sustaining the world's most powerful military force remains expensive and vulnerable to fraud, waste and mismanagement. In FY 1999, the DoD bought about $140 billion in goods and services, in 14.8 million purchasing actions, which means 57,000 purchasing actions on an average working day. Statistics for FY 2000 are not yet available, but will be similar. The scope, complexity, variety and frequent instability of Defense acquisition programs pose particularly daunting management challenges. No major acquisition cost reduction goals have yet been achieved and the results of most of the specific initiatives are still to be determined, particularly since many have not yet been fully implemented and are in a developmental or pilot demonstration phase.

In the rush to streamline and incorporate commercial practices and products, the Department cannot compromise its insistence on quality products and services at fair and reasonable prices. An inherent challenge throughout the Department's acquisition reform effort is ensuring that critically needed controls remain in place and there is proper oversight and feedback on new processes. Recent audits continued to indicate a lack of effective means for identifying best commercial practices and adapting them to the public sector; overpricing of spare parts; inattention to good business practices and regulations when purchasing services; poor oversight of the several hundred medium and small acquisition programs; and adverse consequences from cutting the acquisition workforce in half without a proportional decrease in workload.

It should be axiomatic that each reform initiative needs periodic evaluation, based on quantifiable performance measures, and fine-tuning. There is a tendency, however, for initiatives to be put into place without explicit provision for periodic and objective review. For example, in 1994 the DoD mandated the use of an open systems approach in the acquisition process to reduce the cost of ownership of weapons systems while increasing

competition, interoperability and useful life. We reported in June 2000 that, of 17 major weapon acquisition programs approved at key development milestones between March 1996 and July 1999, 14 programs lacked clearly defined open system design objectives or a strategy for achieving such objectives. In addition, DoD guidance did not require program managers to assess the impact of a given level of design systems. The problems in implementing this particular initiative are typical of those to be expected in mandated reforms that may not be adequately understood, fully supported or enforced over time.

Although the DoD must continue to address the challenge of how to control the cost of purchased goods and services, the most fundamental acquisition issues confronting the Department relate to requirements and funding. The expanding national dialogue on military missions, the pending Quadrennial Defense Review and the ideas of a new administration and Congress could significantly alter DoD missions, military force structure and acquisition requirements. Whether changes in requirements are major or minor, there needs to be a far-reaching rebalancing of acquisition programs to match available funding. In addition, it does not appear that measures taken during the 1990's to provide more stability in acquisition program funding were effective.

Finally, we believe that the Department needs to put more acquisition reform emphasis on ensuring the quality, serviceability and safety of purchased equipment, parts and supplies. Concentrating on prices and timely delivery is vital, but quality should be the most important attribute for DoD purchases, especially for materiel used by the warfighters.

Most Significant Recent Reports on Acquisition

D-2000-65, Costs Charged to Other Transactions, 12/27/99

D-2000-79, Summary of DoD Process for Developing Quantitative Munitions Requirements, 2/24/00

D-2000-88, DoD Acquisition Workforce Reduction Trends and Impacts, 2/29/00

D-2000-100, Contracts for Professional, Administrative and Management Support Services, 3/10/00

Testimony to Subcommittee on Government Management Information and Technology, House Committee on Government Reform, on Defense Acquisition Management, 3/16/00

D-2000-105, Contracting for Anthrax Vaccine, 3/22/00

Testimony to Senate Armed Services Committee on Defense Acquisition, 4/26/00

D-2000-149, Use of an Open Systems Approach for Weapon Systems, 6/14/00

D-2000-174, V-22 Osprey Joint Advanced Vertical Aircraft, 8/15/00

D-2000-187, The Low-Rate Initial Production Decision for the Joint Biological Point Detection System, 9/11/00

D-2000-192, Results of the Defense Logistics Agency Strategic Supplier Alliance for Catalog Items, 9/26/00

D-2001-004, Disposal of Excess Government-Owned Property in the Possession of Contractors, 10/13/00

D-2001-12, Acquisition of the Armored Medical Evacuation Vehicle, 11/22/00

Open Recommendations. The most significant open IG, DoD, recommendations on Acquisition are as follows:

1. To provide better oversight of weapon system acquisition programs, the Department of the Army should designate the Army Acquisition Executive, not lower ranking officials, as the Milestone Decision Authority for Acquisition Category II programs. (Report D-2000-187, 9/11/00)

2. To improve implementation of DoD policy on using open weapon system design approaches, we recommended that the Under Secretary of Defense (Acquisition, Technology and Logistics) enforce the requirement that program managers fully consider the use of open system design techniques. We also recommended that program managers be required to include open system objectives in test and evaluation master plans and to demonstrate their open system approach at milestone decisions. Additionally, we recommended that the Joint Task Force provide program managers with general templates for inserting open systems design language in the key acquisition planning documents and provide guidance to help program managers document the means for determining the extent of system design openness. (Report D-2000-149, 6/14/00)

3. To address widespread deficiencies in contracting practices in contracts for services, we recommended that the Deputy Under Secretary of Defense (Acquisition Reform) develop training on defining requirements for contracts for professional, administrative and management support services; train contracting and program personnel in the

award and administration of contracts for these services; and emphasize, in that training, the need to avoid the kinds of deficiencies noted in our audit report. We also recommended that Senior Acquisition Executives for the Army, Navy, and Air Force establish centers of excellence with trained and experienced personnel that can be used by acquisition personnel when procuring services, make all acquisition personnel aware of the problems identified in our report, and develop a time-based plan with goals and performance measures to determine improvements in the acquisition of professional, administrative and management support services. (Report D-2000-100, 3/10/00)

4. To decrease the risk of continued overpricing of spare parts on sole-source contracts when certified cost or pricing data are not obtained, we recommended that the Defense Logistics Agency attempt to expand its successful strategic supplier approach. (Report D-2000-098, 3/8/00)

5. To address the systemic problems indicated in numerous audit reports on DoD processes for determining munitions requirements, we recommended that the Under Secretary of Defense (Acquisition, Technology and Logistics) and the Joint Staff designate a central authority for updating guidance and overseeing its implementation. The oversight responsibility must extend to assessing and validating the currency of planning scenarios and munitions utilization factors used to quantify requirements. (Report D-2000-079, 2/24/00)

6. To improve management of agreements other than contracts and grants for prototype projects, we recommended that the Directors, Defense Research and Engineering and Defense Procurement, issue "other transaction" guidance in DoD directives, instructions, or regulations. The guidance should preclude the use of Government-funded research as contractor cost share; provide for reasonable use charge of contractor assets; identify how to design an access to records clause; identify the roles and responsibilities of the Defense Contract Audit Agency; provide agreement officers' training on the effects of independent research and development reimbursement on contractor cost share; require agreement officers to inform the administrative contracting officer and the Defense Contract Audit Agency of the award of an other transaction for their review for potential inconsistent accounting treatment of cost shares; and require contractors to use DoD-approved overhead rates when available. In addition, reports to Congress for other transactions should show the effect of independent research and development reimbursements on contractor cost share. (Report D-2000-065, 12/27/99)

7. To address issues related to the impact on competition of using multiple award task order contracts, we recommended that the Director, Defense Procurement, reconsider the need for a guaranteed minimum for every contract awardee and issue additional guidance. (Report 99-116, 3/31/99)

8. To avoid overpricing, we recommended a variety of Defense Logistics Agency contracting actions. (Report 99-026, 10/30/98)

9. To determine whether legal violations occurred in the procurement of certain clothing and textiles, we recommended a series of Anti-Deficiency Act investigations, which will entail an Office of General Counsel determination on whether Buy American Act and Berry Amendment restrictions apply to DoD purchases of commercial items. (Report 99-023, 11/1/99)

10. To ensure proper controls, we recommended the issuance of revised guidance on requesting waivers from weapon system live fire testing and on identifying candidates for testing. (Report 97-214, 9/9/97)

11. To achieve a more effective program for acquiring foreign weapons and other material for testing, we recommended that the Under Secretary of Defense (Acquisition, Technology and Logistics) issue new prioritization guidance. (Report 97-133, 4/21/97)

12. To revitalize the Value Engineering Program, we recommended that the Under Secretary of Defense (Acquisition, Technology and Logistics) issue new guidelines on using Value Engineering and reporting savings. (Reports 97-121, 4/9/97 and 97-3, 10/9/96)

Closed Recommendations. The most significant of our recently closed recommendations in this area are as follows.

1. To enable evaluation of the impact of emphasizing the procurement of more commercial items, the Defense Logistics Agency (DLA) collected price trend data from the inventory control points. The Military Departments need to emulate DLA so that the DoD and Congress have reliable information on the outcome of acquisition reforms. (Report 98-88, 3/11/98)

2. To improve coordination and management control, the Military Departments and Ballistic Missile Defense Organization issued guidance on management of aerial target systems. (Report 92-20, 12/31/91)

3. To achieve cost reductions, the Theater High Altitude Area Defense Program implemented a multi-year procurement strategy and component breakout for competition. (Report 96-14, 10/23/95)

4. To avoid problems with Foreign Military Sales customers, regulations were changed to require longer records retention periods after case closure. (Report 95-304, 9/11/95)

Health Care

The Challenge. The Military Health System (MHS) costs over $16 billion annually and serves approximately 8.2 million eligible beneficiaries through its health care delivery program, TRICARE. TRICARE provides health care through a combination of direct care at Military Department hospitals and clinics and purchased care through managed care support contracts. The MHS has dual missions to support wartime deployments (readiness) and provide health care during peacetime.

The MHS faces three major challenges: cost containment, transitioning to managed care, and data integrity. These challenges are complicated by the inadequate information systems available to support the MHS.

Cost containment within the MHS is challenged by the continued lack of good cost information combined with significant levels of health care fraud. Lack of comprehensive patient-level cost data has made decisions regarding whether to purchase health care or to provide the care at the military treatment facility more difficult. Recent legislation, which expands medical benefits for military retirees to include pharmaceuticals, will entail considerable program growth in an area where cost control has been difficult. Past audits have questioned the efficiency of duplicative pharmaceutical procurements by DoD and the Department of Veterans Affairs.

Data integrity in management information systems has been a persistent problem that affects both health care program effectiveness and efficiency. The lack of complete and accurate data has resulted in an inability to clearly identify health care costs, identify unit and individual readiness for deployment, or coordinate direct health care with purchased health care. The DoD management has put considerable emphasis on improved data quality and significant progress is being made.

To combat health care fraud, the Defense Criminal Investigative Service has developed an active partnership with the TRICARE Management Activity to give high priority to health care fraud cases, which comprise a growing portion of the overall investigative workload. As of September 30, 2000, we had 521 open criminal cases in this area.

Transitioning to managed care is a critical element in peacetime health care delivery. The issue is complicated by a lack of understanding about TRICARE, multiple TRICARE programs offering similar but not identical benefits, and increased focus on providing peacetime health care to the aging retiree population. An audit of the TRICARE marketing program in 1999 showed that,

while the level of beneficiary understanding of TRICARE was increasing, DoD had provided Service members with incomplete, incorrect, or inconsistent information. In addition, with increased base and hospital closures and military downsizing, more and more older beneficiaries (those eligible for Medicare but not DoD-purchased health care) find themselves without accessibility to direct care resources. Attempts to address that problem have led to a proliferation of health care demonstration programs that have further confused the eligible population.

Most Significant Recent Reports and Testimony on Health Care

Testimony to the Subcommittee on Oversight and Investigations, House Committee on Veterans Affairs, on Procuring Pharmaceuticals for the Department of Defense, 5/25/00.

Open Recommendations. Audit coverage has been severely limited in the area of Health Care for the past several years. The most significant open IG, DoD, recommendations on this subject are as follows:

1. To improve user acceptance of TRICARE, we recommended issuing clear requirements for a comprehensive national TRICARE marketing program. (Report 00-016, 10/21/99)

2. To avoid duplicate payments for care provided in medical treatment facilities to retired individuals enrolled in Medicare health maintenance organizations, we recommended that DoD and the Department of Health and Human Services develop a strategy and propose any necessary legislation. (Report 99-152, 5/28/99)

3. To achieve greater efficiency and lower costs in procuring pharmaceuticals, we recommended that the DoD and Department of Veterans Affairs merge their procurement processes. (Report 98-154, 6/15/98)

4. To address deficiencies in medical war reserves in Korea, we recommended completing a Medical Logistics Interservice Support agreement. (Report 97-170, 6/16/97)

Closed Recommendations. The most significant of our recently closed recommendations in this area are as follows.

1. To enable better management of DoD graduate medical education programs, system changes have been implemented to provide good cost visibility. (Report 97-147, 5/23/97)

2. To eliminate discounts that had the effect of encouraging smoking and driving up DoD health care costs, policy was issued to make commissary and exchange retail prices for tobacco products consistent with commercial prices. (Report 97-60, 12/31/96)

Supply Inventory Management

The Challenge. Supply management to support U.S. military forces, which are located around the world and use several million different types of weapon systems, other equipment, spare parts, fuel, apparel, food items, pharmaceuticals and other supplies, may be the most difficult logistics challenge in the world. Despite the clear need to modernize DoD supply operations, it should be noted that U.S. military logistics performance has been excellent in demanding situations such as the Gulf War and the numerous recent deployments to comparatively remote areas of the world.

Every facet of supply management involves challenges and it is critically important to recognize that weapon systems and other equipment must be designed, selected and procured with logistics support as a paramount concern. The use of standardized parts, commercial items, non-hazardous materials and easy to maintain components will considerably ease the supply support problem for each system or piece of equipment. Conversely, inattention to such factors during acquisition will increase the risk of higher costs and logistics failures. The logistics community relies heavily on program managers and operators to help forecast supply requirements, and historically this has been very difficult. The Department has been justifiably criticized for accumulating excessive supply inventories, but supply shortfalls are at least as great a concern due to the impact on readiness. Current logistics reform initiatives are principally focused on introducing private sector logistics support practices, which in turn are based on applying web-based technology. The DoD has initiated a myriad of logistics improvement initiatives, most of which are still in early stages. We anticipate continuing valid concerns about all phases of supply support, including requirements determination, procurement, distribution, and disposal.

Most Significant Recent Reports on Supply Inventory Management

D-2000-086, Assuring Condition and Inventory Accountability of Chemical Protective Suits, 2/25/00

D-2000-113, Required Delivery Dates in Requisitions for Secondary Items of Supply Inventory, 4/19/00

D-2000-147, DoD Pilot Program for Shipment of Personal Property - Military Traffic Management Command Reengineering DoD Personnel Property Program Pilot, 6/12/00

D-2000-171, Reacquisition of Surplus Materiel by the Defense Logistics Agency, 8/9/00

D-2000-185, Allegations to the Defense Hotline Concerning Management of Obsolete Reparable Items, 9/7/00

D-2001-2, Defense Logistics Agency Customer Returns Improvement Initiative Program, 10/12/00

D-2001-4, Disposal of Excess Government-Owned Property in the Possession of Contractors, 10/13/00

Open Recommendations. The most significant open IG, DoD, recommendations in the area of Supply Inventory Management are as follows:

1. To ensure that poor quality materiel identified by users is removed from active inventory and other appropriate action is taken, we recommended that the Defense Logistics Agency fully implement the Customer Returns Improvement Initiative Program at all distribution depots. (Report D-2001-002, 10/12/00)

2. Military units and other organizations designate Required Delivery Dates (RDD) on supply requisitions. To improve the appropriate use of RDD information by personnel involved in preparing or filling supply requisitions, we recommended that the Assistant Deputy Under Secretary of Defense (Supply Chain Integration) streamline the number of RDD categories. We recommended that the Department of the Army improve awareness of the importance of RDD, streamline rules for their use, and provide training. We also recommended Defense Logistics Agency and Army actions to implement automated edit of RDD. (Report D-2000-113, 4/19/00)

3. To reengineer the DoD property disposal process, we recommended a comprehensive reworking of management controls for all facets of the disposal process, which should result in a plan addressing controls, training, management information and performance measurement. (Report 99-029, 11/31/98)

4. To improve efficiency, we recommended that there be standard DoD-wide procedures for contractors to report the return of repairable assets from DoD users to contractor repair facilities. (Report 97-014, 11/1/96)

5. To improve asset management, we recommended that the Services take measures to enhance the visibility that Primary Inventory Control Activities have over materiel at the Secondary Inventory Control Activities, so that purchases of items already in stock are minimized and good redistribution decisions are feasible. (Report 95-303, 9/1/95)

Closed Recommendations. The most significant of our recommendations that were recently closed in this area are as follows:

1. To accelerate the disposal of obsolete material in the Defense National Stockpile, the Defense Logistics Agency developed an aggressive sales strategy that increased sales from $446 million in FY 1999 to $670 million in FY 2000. (Report 99-044, 12/3/98)

2. To eliminate under charging Foreign Military Sales customers with Cooperative Logistics Supply Support Arrangements, the Military Departments addressed 99 percent of the $140 million in under billing identified by auditors. (Report 95-31, 11/21/94)

Other Infrastructure Issues

The Challenge. Despite numerous management initiatives to reduce support costs so that more funds could be applied to recapitalizing and ensuring the readiness of military forces, more can and should be done. The number of bases and other installations remains excessive, justifying at least one more round of base closures and realignments. Organizations throughout the Department need to continue reengineering their business processes and striving for greater administrative efficiency.

Unfortunately, cutting support costs can easily become counterproductive if the quality of support services and facilities is degraded. In addition, there are numerous bona fide requirements in the support area that will be expensive to address. For example, the DoD urgently needs to replace at least one third of its housing units over the next few years. The resulting $30 to $40 billion cost will compete in the budget against other recapitalization needs. Finally, DoD has one of the largest environmental restoration programs in the world and this area is particularly challenging in terms of cost containment and compliance with continually evolving laws and regulations. During the past year, incidents such as the outcry in Korea over the spill of chemicals from a U.S. facility have underscored the growing international dimension of the DoD environmental challenge.

Most Significant Recent Reports on Other Infrastructure Issues

D-2000-121, Hazardous Material Management for Major Defense Systems, 5/4/00

D-2000-127, Program Management of the Materials and Processes Partnership for Pollution Prevention, 5/22/00

D-2000-157, DoD Hazardous Waste Management and Removal Services in the U.S. European Command, 6/28/00

D-2000-170, Disposal of Range Residue, 8/4/00

D-2000-175, Defense Information Systems Agency Right-Sizing Plan for Regional Support Activities, 8/15/00

Open Recommendations. Significant open recommendations in this area include the following:

1. To address hazardous conditions related to munitions residue on DoD training and test ranges, we recommended 25 actions in Report 97-213, 9/5/97. A follow-up audit indicated

little or no action on 10 of those 25 agreed-upon recommendations, which we have reiterated. (Report 2000-170, 8/4/00)

2. To control the risk of poor performance by environmentally hazardous waste disposal contractors for U.S. European Command components, we recommended a variety of actions by the Military Departments and the Defense Logistics Agency. (Report D-2000-157, 6/28/00)

3. To ensure close attention to weapon system life cycle costs driven by hazardous material handling and disposal requirements, we recommended that acquisition program managers comply fully with DoD policies encouraging focus on those requirements early in the acquisition cycle. (Report D-2000-121, 5/4/00)

4. To establish a more reliable process for estimating unaccompanied personnel housing requirements, we recommended using a standard form and methodology. (Report 99-239, 10/8/99)

5. To address problems in assessing family housing requirements, we recommended developing a standardized process. (Report 98-6, 10/8/97)

6. To improve efficiency, we recommended enhanced systems and controls for the DoD Personal Property Shipment and Storage Program. (Report 97-175, 6/23/97)

Closed Recommendations. The most significant of our recommendations in this area that were recently closed are as follows:

1. To calculate future unaccompanied enlisted personnel housing requirements more accurately, the Navy adjusted its computer model and related guidance to reflect the new barracks construction standard. (Report 98-80, 2/23/98)

2. To eliminate environmental hazards caused by lead contamination, the Army Reserve closed its indoor firing ranges and the Army National Guard took steps to reduce risks. (Report 98-170, 6/30/98)

3. To avoid friction with the host government and protect U.S. personnel from personal liability in environmental disputes, the Army developed training on the implications of the 1993 Supplementary Status of Forces Agreement with Germany. (Report 99-251, 9/15/99)

Readiness

The Challenge. Concern about the readiness of U.S. military forces was a principal issue in congressional hearings and was addressed during the Presidential election campaign. There is a fairly broad consensus that readiness shortfalls exist, although the extent of impairment to mission capability is more contentious. Clearly, there are spare parts shortages; significant backlogs for depot maintenance ($1.2 billion) and real property maintenance ($27.2 billion); concerns related to recruiting, retention and morale; disproportionately numerous deployments for some units; unanticipatedly high operating tempo; and equipment availability problems. The DoD and Congress have made budget adjustments and military entitlements have been expanded. The Department's readiness posture ultimately depends, however, on the effectiveness of hundreds of support programs, which range from training to supply management.

The DoD audit community supported the successful program to overcome the Year 2000 computer challenge, which the Department considered to be a major readiness issue, with the largest audit effort in DoD history. The IG, DoD, issued 185 "Y2K" reports. Due to that massive commitment, resource constraints and other workload, our recent coverage of other readiness issues was severely limited. We plan to restore at least some of the necessary coverage during FY 2001, continuing our particular concentration on chemical and biological defense issues.

Most Significant Recent Reports and Testimony on Readiness

D-2000-086, Assuring Condition and Inventory Accountability of Chemical Protective Suits, 2/25/00

Testimony to Subcommittee on National Security, Veterans Affairs and International Relations, House Committee on Government Reform, 6/21/00

Open Recommendations. The most significant open recommendations related to Readiness are as follows:

1. To ensure that war reserves are adequate to support medical material requirements in a dual major war contingency, we recommended a comprehensive review of DoD surge capacity and measures to ensure the availability of medical items. (Report 99-201, 10/26/99)

INTERNET DOCUMENT INFORMATION FORM

A . Report Title: Program Management of the Defense Security Service Case Control Management System

B. DATE Report Downloaded From the Internet: 12/20/00

C. Report's Point of Contact: (Name, Organization, Address, Office Symbol, & Ph #): **OAIG-AUD (ATTN: AFTS Audit Suggestions)**
Inspector General, Department of Defense
400 Army Navy Drive (Room 801)
Arlington, VA 22202-2884

D. Currently Applicable Classification Level: Unclassified

E. Distribution Statement A: Approved for Public Release

F. The foregoing information was compiled and provided by:
DTIC-OCA, Initials: __VM__ **Preparation Date 12/20/00**

The foregoing information should exactly correspond to the Title, Report Number, and the Date on the accompanying report document. If there are mismatches, or other questions, contact the above OCA Representative for resolution.